Unit B3
Permutations

Introduction

In this unit you will study groups whose elements are *permutations*. You will see that these provide us with an abundant supply of finite groups.

A *permutation* of a finite set is a function that rearranges the elements of the set. You have already met examples of permutations in this book: each two-line symbol representing a symmetry of a figure specifies a permutation of the set of location labels of the figure, since the bottom line of each two-line symbol indicates how the labels in the top line are rearranged. In this unit you will meet another notation for permutations, called *cycle form*, which is often more convenient. You will learn how to compose and find inverses of permutations written in this form, and you will see that the set of all permutations of a set of n elements forms a group under function composition.

You will go on to study some properties of permutations, and consider various subgroups of the group of all permutations of n symbols. You will also explore the idea of using one permutation to rename the symbols in another permutation, an idea that leads to the important concept of *conjugacy*.

At the end of the unit you will meet Cayley's Theorem, a result that highlights the importance of permutations in group theory. It asserts that every finite group is isomorphic to (and therefore essentially the same as) a group of permutations.

1 Permutations

In this section you will be introduced to the idea of a permutation, see how to write permutations in cycle form, and learn how to compose and invert them in this form.

1.1 Cycle form of a permutation

We begin with a definition of what we mean by a *permutation* in group theory.

Definition

A **permutation** of a finite set S is a one-to-one function from S to S.

So a permutation is a function that maps each element of a finite set to an element of the same set, in such a way that each element of the set is used exactly once as an image, as illustrated for a 5-element set in Figure 1 (there must be exactly one arrow from and to each element). Note that a function from a finite set to itself that is one-to-one must also be onto.

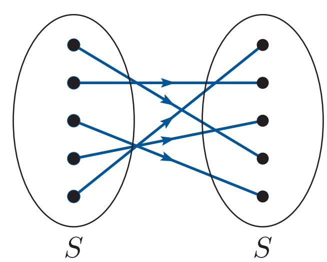


Figure 1 A permutation of a 5-element set S

We usually work with permutations of sets of the form

$$\{1, 2, 3, \ldots, n\},$$

where n is a natural number. Examples of such sets include $\{1, 2, 3\}$ and $\{1, 2, 3, 4\}$. We refer to the elements of the set as the **symbols** being permuted.

A simple way of specifying a permutation is to list the symbols being permuted on one line, and the corresponding image of each symbol underneath it on a second line, enclosing the whole array in brackets. An example of a permutation of the set $\{1, 2, 3, 4, 5, 6\}$ written in this way is

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

This permutation f maps the symbols 1 to 5, 2 to 6, 3 to 1, and so on, as we see by reading downwards.

We call this notation the **two-line form** of a permutation. The format is the same as that of the *two-line symbols* that we used to represent symmetries in Units B1 and B2, and indeed those are all examples of permutations.

You may previously have seen the word 'permutation' used in a different but related sense, to mean an arrangement of the elements of a finite set. This is its usual meaning in the field of mathematics known as *combinatorics*. When used in this sense, a permutation does not mean a one-to-one function from a finite set to itself, but it can be thought of as the *result* of applying such a function to a list of the elements of the set, because the effect of the function is to rearrange the list. For example, the bottom row of the two-line form above is a permutation, in the combinatorial sense, of the symbols in the top row. In group theory we always use the word permutation to mean the *function* itself, as in the definition above, rather than the resulting rearrangement of the elements of the set.

There is another notation for permutations, an alternative to two-line form, which is often more convenient. Consider again the permutation f given in two-line form above. If we start at the symbol 1 and apply f repeatedly, then we get the string of symbols

$$1 \xrightarrow{f} 5 \xrightarrow{f} 4 \xrightarrow{f} 2 \xrightarrow{f} 6 \xrightarrow{f} 3 \xrightarrow{f} 1.$$

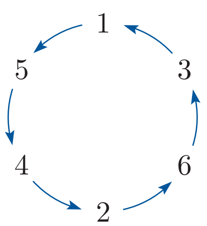


Figure 2 A cycle of six symbols

This string contains all the information needed to specify f, since it gives the image under f of each of the six symbols being permuted. It shows that f permutes the six symbols in the **cycle** shown in Figure 2.

We can use this fact to provide a more concise notation for f than the two-line form above. We write

$$f = (1\ 5\ 4\ 2\ 6\ 3),$$

with the interpretation that f maps each symbol to the one immediately to the right of it, and maps the last symbol back to the first (in this case,

3 maps to 1). We call this the *cycle form* of f. As the cycle has no particular starting point, we can write any of the symbols first. For example, we can write

$$f = (4\ 2\ 6\ 3\ 1\ 5) \quad \text{and} \quad f = (3\ 1\ 5\ 4\ 2\ 6);$$

these convey exactly the same information and are equally good representations of f. However, when the symbols being permuted are numbers, we usually write the smallest number first in a cycle unless there is a reason to do otherwise.

Exercise B81

(a) Write down the cycle form of each of the following permutations.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 6 & 2 & 1 & 4 \end{pmatrix}$

(b) Write down the two-line form of each of the following permutations given in cycle form.

(i) $(1\ 3\ 2)$ (ii) $(1\ 6\ 2\ 4\ 3\ 5)$

(c) Can you write down a cycle corresponding to the following permutation g? If not, why not?

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 1 & 2 & 7 & 5 \end{pmatrix}$$

Not all permutations can be written in cycle form as simply as our first example f, because not every permutation maps all the symbols in a single cycle. For example, for the permutation

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 1 & 2 & 7 & 5 \end{pmatrix}$$

in Exercise B81(c) we have

$$1 \xrightarrow{g} 4 \xrightarrow{g} 3 \xrightarrow{g} 8 \xrightarrow{g} 5 \xrightarrow{g} 1,$$

and we can write this string as the cycle $(1\ 4\ 3\ 8\ 5)$. But what about the other symbols? Starting at the symbol 2 we have

$$2 \xrightarrow{g} 6 \xrightarrow{g} 2,$$

which gives the cycle $(2\ 6)$. Also we have the symbol 7, which is mapped to itself:

$$7 \xrightarrow{g} 7.$$

We can represent this by the 'short cycle' (7).

Thus g is made up of three disjoint cycles, as shown in Figure 3. We say that two or more cycles are **disjoint** if each symbol that appears in the cycles appears in only one cycle.

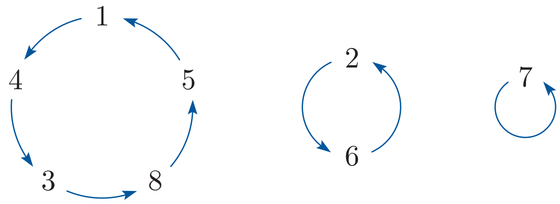


Figure 3 The cycles of the permutation g

We write the permutation g as

$$g = (1\ 4\ 3\ 8\ 5)(2\ 6)(7).$$

We call this the *cycle form* of g and say that g is the **product** of the disjoint cycles $(1\ 4\ 3\ 8\ 5)$, $(2\ 6)$ and (7). As before, the starting point of each cycle does not matter. Also, because the three cycles are disjoint, it makes no difference if we write them in a different order. Thus we can convey the same information by writing, for example,

$$g = (6\ 2)(7)(3\ 8\ 5\ 1\ 4) \quad \text{or} \quad g = (7)(5\ 1\ 4\ 3\ 8)(2\ 6).$$

Exercise B82

Complete the following cycle forms for the permutation g above.

(a) $g = (7)(8 - \ - \ - \ -)(6\ -)$ (b) $g = (5 - \ - \ - \ -)(2\ -)(-)$

In general, we say that a permutation is written in **cycle form** when it is written as a product of disjoint cycles.

When the symbols being permuted are numbers, we usually write the cycle form of a permutation with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order, unless there is a reason to do otherwise. For example, we would usually write the permutation g above as

$$g = (1\ 4\ 3\ 8\ 5)(2\ 6)(7).$$

Here 1, 2 and 7 are the smallest numbers in their respective cycles, so they appear first in the cycles, and the cycles containing 1, 2 and 7, respectively, appear in that order.

The cycle form of any permutation can be found by carrying out a procedure similar to that used above for the permutation g, as outlined in the following strategy.

Strategy B7

To find the cycle form of a permutation f, do the following.

1. Choose any symbol (such as 1) and find its image under f, then find the image of its image under f, and so on, until you encounter the starting symbol again.
2. Write these symbols as a cycle.
3. Repeat the process starting with any symbol that has not yet been placed in a cycle, until all the symbols have been placed in cycles.

When you use Strategy B7, it does not matter which symbol you choose to start each new cycle, as long as it is one that you have not yet placed in a cycle. However, if the symbols are numbers, and you always choose the smallest number not yet placed in a cycle, then you will automatically obtain the cycle form of the permutation written in the usual way described above (that is, with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order). This is demonstrated in the worked exercise below.

Worked Exercise B32

Find the cycle form of the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 7 & 5 & 3 & 4 \end{pmatrix}.$$

Solution

Start the first cycle with the smallest symbol, 1. This gives $1 \longrightarrow 6 \longrightarrow 3 \longrightarrow 1$.

$$f = (1\ 6\ 3)\ldots.$$

Start the next cycle with the smallest symbol not yet placed in a cycle, which is 2. This gives $2 \longrightarrow 2$.

$$f = (1\ 6\ 3)(2)\ldots.$$

Continue in the same way to obtain the remaining cycles. This gives $4 \longrightarrow 7 \longrightarrow 4$ and $5 \longrightarrow 5$.

$$f = (1\ 6\ 3)(2)(4\ 7)(5).$$

All the symbols have now been placed in cycles, so the cycle form is complete.

You may have wondered how we can be sure that we will eventually encounter the starting symbol again in step 1 of Strategy B7. To see why this is, first note that because there are only finitely many symbols, at some point we must encounter again some symbol that we have encountered before. Let x be the first symbol that we encounter twice. If x were not the symbol that we started with, then x would be the image under f of two different symbols (the symbols encountered immediately before the two occurrences of x), and this cannot happen because f is one-to-one.

Exercise B83

(a) Convert the following permutations from two-line form to cycle form.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 1 & 5 & 3 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 9 & 1 & 3 & 8 & 2 & 6 & 4 \end{pmatrix}$

(b) Convert the following permutations from cycle form to two-line form.

(i) $(1\ 6)(2\ 3\ 7\ 5)(4)$ (ii) $(1\ 6\ 4\ 2)(3\ 5\ 8)(7)$

Since Strategy B7 can be applied to any permutation, and since it must always give the same cycles for any particular permutation, we have the following result.

Theorem B51

Every permutation can written in cycle form. The cycle form of a permutation is unique, apart from the choice of starting symbol in each cycle and the order in which the cycles are written.

When a cycle of a permutation consists of a single symbol, the permutation maps that symbol to itself. We say that the symbol is **fixed** by the permutation. For example, the permutation

$$f = (1\ 6\ 3)(2)(4\ 7)(5)$$

fixes both the symbols 2 and 5.

Usually, we omit cycles containing a single symbol from the cycle form of a permutation. For example, if it is clear from the context that the permutation f above permutes the symbols of the set $\{1, 2, 3, 4, 5, 6, 7\}$, then we write

$$f = (1\ 6\ 3)(4\ 7),$$

and it is understood that the missing symbols 2 and 5 are fixed by f.

Exercise B84

Convert the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 4 & 8 & 3 & 6 & 1 & 5 \end{pmatrix}$$

from two-line form to cycle form, omitting any cycles that contain a single symbol from the final cycle form.

The **identity permutation** of a set S is the permutation of S that fixes every symbol. For example, the identity permutation of the set $S = \{1, 2, 3, 4, 5, 6, 7\}$ has the two-line form

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

The cycle form of this permutation can be written as

$$(1)(2)(3)(4)(5)(6)(7).$$

Unfortunately, if we omit the cycles containing a single symbol from this cycle form, then there is nothing left! For this reason, when we work with cycle forms, we usually denote the identity permutation simply by e.

The two conventions described above are summarised in the box below.

Cycle form conventions

- When it is clear from the context which set of symbols is being permuted, we omit fixed symbols from the cycle form of a permutation.
- When working with permutations in cycle form, we denote the identity permutation by e.

Exercise B85

Write down the two-line form of each of the following permutations of $\{1, 2, 3, 4, 5\}$.

(a) $(1\ 4)(2\ 5)$ (b) $(1\ 2)$ (c) $(1\ 5\ 4)$ (d) e

The notations that we call the two-line form and the cycle form of a permutation were both introduced by the French mathematician Augustin-Louis Cauchy (1789–1857), in two major papers in which he launched the subject of permutations as an independent area of study. The two-line form appeared in the paper of 1815, and the cycle form appeared nearly 30 years later in the paper of 1844.

Augustin-Louis Cauchy

1.2 Composing permutations

A composite of two permutations is a permutation, because if f and g are functions that map a set S to itself, then so does $g \circ f$; and if f and g are both one-to-one, then so is $g \circ f$.

In Unit B1 *Symmetry* you saw how to compose two symmetries written as two-line symbols; we can use the same method to compose any two permutations written in two-line form. However, when we want to compose two permutations that are written in cycle form, we can do so without having to first convert them to two-line form, as demonstrated in the next worked exercise.

Worked Exercise B33

Let $f = (1\ 4\ 3)(2\ 6)$ and $g = (1\ 4\ 6\ 2\ 5)$ be permutations of $\{1, 2, 3, 4, 5, 6\}$. Find the cycle form of $g \circ f$.

Solution

Write down the cycle forms of f and g, in the right order.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6)$$

Remember that, as f and g are functions, the composite permutation $g \circ f$ means 'first f, then g'. Start the first cycle of $g \circ f$ with the smallest symbol, 1.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1 \ldots$$

Find the image of 1 under $g \circ f$. We see that f (the first permutation) maps 1 to 4, then g maps 4 to 6:

$$\begin{tikzcd} 1 \arrow[r, "f"'] \arrow[rr, bend left, "g \circ f"] & 4 \arrow[r, "g"'] & 6 \end{tikzcd}$$

So $g \circ f$ maps 1 to 6.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6 \ldots$$

To continue the cycle, find the image of 6. We see that f maps 6 to 2, then g maps 2 to 5, so $g \circ f$ maps 6 to 5.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5 \ldots$$

Continue in the same way. Next we see that f fixes 5, then g maps 5 to 1, so $g \circ f$ maps 5 to 1. Since 1 is the start of the cycle, the cycle is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5) \ldots$$

Now start a new cycle with the smallest symbol not yet placed in a cycle, which is 2.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(\boxed{2} \ldots$$

We see that f maps 2 to 6, then g maps 6 to 2, so $g \circ f$ fixes 2. So this cycle is complete.

$$g \circ f = (1\ 4\ \boxed{6\ 2}\ 5) \circ (1\ 4\ 3)(\boxed{2\ 6}) = (1\ 6\ 5)(\boxed{2}) \ldots$$

Start a new cycle with the smallest symbol not yet placed in a cycle, which is 3.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)(\boxed{3} \ldots$$

To continue the cycle, find the image of 3. We see that f maps 3 to 1, then g maps 1 to 4, so $g \circ f$ maps 3 to 4.

$$g \circ f = (\boxed{1\ 4}\ 6\ 2\ 5) \circ (\boxed{1}\ 4\ \boxed{3})(2\ 6) = (1\ 6\ 5)(2)(\boxed{3\ 4} \ldots$$

Next, we see that f maps 4 to 3, then g fixes 3, so $g \circ f$ maps 4 to 3. Since 3 is the start of the cycle, the cycle is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ \boxed{4\ 3})(2\ 6) = (1\ 6\ 5)(2)(\boxed{3\ 4})$$

All six symbols have now been placed in cycles, so the cycle form is complete.

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6) = (1\ 6\ 5)(2)(3\ 4) = (1\ 6\ 5)(3\ 4).$$

Note that if

$$f = (1\ 4\ 3)(2\ 6) \quad \text{and} \quad g = (1\ 4\ 6\ 2\ 5),$$

as in the worked exercise above, then although it is true that

$$g \circ f = (1\ 4\ 6\ 2\ 5) \circ (1\ 4\ 3)(2\ 6),$$

the expression on the right here is *not a cycle form*, because the cycles are *not disjoint* – some symbols are repeated. The correct cycle form of $g \circ f$ is as found in the worked exercise.

The strategy below summaries the method used in Worked Exercise B33.

Strategy B8

To find the composite $g \circ f$ of two permutations written in cycle form, do the following.

1. Start with the smallest symbol, 1 say. Find the symbol that is the image of 1 under f, then find the image of that symbol under g, and write the result, x say, next to 1 in a cycle:

   $$(1\ x\ \ldots.$$

2. Starting with the symbol x, repeat the process to obtain the next symbol in the cycle.
3. Continue repeating the process until the next symbol found is the original symbol 1. This completes the cycle.
4. Starting with the smallest symbol not yet placed in a cycle, repeat steps 1 to 3 until every symbol has been placed in a cycle.
5. Usually, rewrite the cycle form omitting the cycles containing a single symbol, if there are any.

When you use Strategy B8, it is not strictly necessary to start each new cycle with the *smallest* symbol not yet placed in a cycle – any symbol not yet placed in a cycle will do. However, if you always choose the smallest symbol, then the cycle form you obtain will automatically be written in the conventional way (that is, with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order).

Exercise B86

Let $f = (1\ 4\ 3)(2\ 6)$ and $g = (1\ 4\ 6\ 2\ 5)$ be permutations of $\{1, 2, 3, 4, 5, 6\}$, as in Worked Exercise B33. Use Strategy B8 to determine each of the following permutations in cycle form.

(a) $f \circ g$ (b) $f \circ f$ (c) $g \circ g$

Worked Exercise B33 and Exercise B86(a) illustrate the fact that the order in which two permutations are composed is important: for the permutations f and g here,

$$g \circ f \neq f \circ g.$$

In general, if f and g are permutations, then the composite permutations $g \circ f$ and $f \circ g$ are usually not equal. That is, composition of permutations is not *commutative* (as is true for functions in general).

Exercise B87

Let $f = (1\ 3\ 2\ 4\ 6)$ and $g = (1\ 4)(3\ 5)$ be permutations of $\{1, 2, 3, 4, 5, 6\}$. Determine each of the following permutations in cycle form.

(a) $g \circ f$ (b) $f \circ g$ (c) $f \circ f$ (d) $g \circ g$

Sometimes we need to find a composite of three or more permutations. One way to do this is to deal with the permutations two at a time, using Strategy B8. For example, if you want to find a composite $h \circ g \circ f$, then you can first use Strategy B8 to find $g \circ f$, and then use it again to find $h \circ (g \circ f)$.

However, it is more efficient to deal with all the permutations at the same time, by adapting Strategy B8. This is demonstrated in the next worked exercise.

Worked Exercise B34

Determine the cycle form of the following permutation of the set $\{1, 2, 3, 4, 5, 6\}$:

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6).$$

Solution

Start the first cycle of the composite permutation with the smallest symbol, 1.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1 \ldots$$

Find the image of 1 under the composite permutation. Remember that the permutations are carried out in order *from right to left*. The first permutation maps 1 to 2, the second maps 2 to 4 and the third maps 4 to 6:

$$\begin{tikzcd} 1 \arrow[r] \arrow[rrr, bend left] & 2 \arrow[r] & 4 \arrow[r] & 6 \end{tikzcd}$$

So the composite permutation maps 1 to 6.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6 \ldots$$

To continue the cycle, find the image of 6. The first permutation maps 6 to 4, the second maps 4 to 1 and the third maps 1 to 4, so the composite permutation maps 6 to 4.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4 \ldots$$

Next, find the image of 4. The first permutation maps 4 to 6, the second maps 6 to itself and the third maps 6 to 1, so the composite permutation maps 4 to 1. Since 1 is the start of the cycle, the cycle is complete.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)\ldots$$

Now start a new cycle with the smallest symbol not yet placed in a cycle, which is 2.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ldots$$

Find the image of 2. The first permutation maps 2 to 1, the second maps 1 to 5 and the third maps 5 to 3, so the composite permutation maps 2 to 3.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ldots$$

Continue the cycle by finding the image of 3. The first permutation maps 3 to 5, the second maps 5 to 3 and the third maps 3 to 5, so the composite permutation maps 3 to 5.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ 5\ldots$$

Now find the image of 5. The first permutation maps 5 to 3, the second maps 3 to 2 and the third fixes 2, so the composite permutation maps 5 to 2. Since 2 is the start of the cycle, the cycle is complete.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ 5)$$

All six symbols have now been placed in cycles, so the cycle form is complete.

$$(1\ 4\ 6)(3\ 5) \circ (1\ 5\ 3\ 2\ 4) \circ (1\ 2)(3\ 5)(4\ 6) = (1\ 6\ 4)(2\ 3\ 5)$$

Exercise B88

Determine the cycle form of each of the following permutations of $\{1, 2, 3, 4, 5, 6, 7\}$.

(a) $(1\ 3)(2\ 4)(5\ 7\ 6) \circ (1\ 7\ 6)(2\ 3) \circ (1\ 7\ 4\ 6)$

(b) $(1\ 7\ 3\ 4\ 6) \circ (1\ 2) \circ (3\ 7) \circ (5\ 3)$

It is useful to note that any permutation is equal to the composite of its disjoint cycles. For example, consider the following permutation of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, written in cycle form:

$$f = (1\ 3)(2\ 4\ 9\ 6)(5\ 7\ 8).$$

Each of the three disjoint cycles in this cycle form is a permutation in its own right; for example, (1 3) is the permutation that interchanges the symbols 1 and 3 and leaves all the other symbols fixed. Furthermore, the overall effect of f is the same as the effect of first performing the permutation (5 7 8), then (2 4 9 6) and then (1 3), so f is the composite of these three permutations. That is,

$$f = (1\ 3) \circ (2\ 4\ 9\ 6) \circ (5\ 7\ 8).$$

In fact, since these three permutations are disjoint cycles, f is their composite *in any order*. We will use the fact that any permutation is equal to the composite of its disjoint cycles later in the unit.

In many texts on group theory, a composite of permutations is called a *product* of permutations, and, accordingly, the operation of forming such a composite is denoted by juxtaposition rather than by the symbol $\circ$. (To **juxtapose** objects is to place them next to each other.) For example, the composite $(1\ 2\ 3)(4\ 5) \circ (2\ 4)$ of the two permutations (2 4) and (1 2 3)(4 5) would be denoted simply by (1 2 3)(4 5)(2 4).

In this module, however, we reserve the word 'product' for composites of disjoint cycles, and we usually retain the use of the symbol $\circ$ for the operation of composition of permutations.

1.3 Finding the inverse of a permutation

Since every permutation f is a one-to-one function, it has an inverse function f^{-1}, which we call the **inverse permutation** of f.

You have seen that every permutation f is made up of disjoint cycles. Since the inverse f^{-1} of f undoes what f does – that is, if f maps x to y, then f^{-1} maps y to x – it follows that f^{-1} is obtained from f by reversing the direction of the disjoint cycles of f.

For example, consider the permutation f whose disjoint cycles are shown in Figure 4(a). The disjoint cycles of its inverse f^{-1} are shown in Figure 4(b).

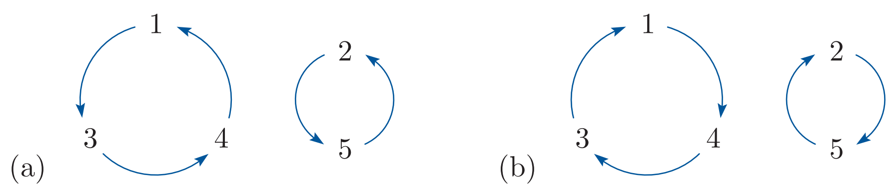


Figure 4 (a) The cycles of a particular permutation f (b) The cycles of f^{-1}

So we have the following strategy for finding the inverse of a permutation written in cycle form. It is illustrated in the worked exercise below for the permutation f in Figure 4.

Strategy B9

To find the inverse of a permutation written in cycle form, do the following.

1. Reverse the order of the symbols in each cycle.
2. Then, usually, rewrite each cycle so that the smallest symbol is first.

Worked Exercise B35

Determine the inverse of the following permutation of $\{1, 2, 3, 4, 5\}$:

$$f = (1\ 3\ 4)(2\ 5).$$

Solution

Reverse the order of the symbols in each cycle.

$$f^{-1} = (4\ 3\ 1)(5\ 2)$$

Rewrite each cycle with the smallest symbol first.

$$= (1\ 4\ 3)(2\ 5)$$

You can confirm that the inverse permutation found in Worked Exercise B35 is correct by checking that $f \circ f^{-1} = e = f^{-1} \circ f$, that is,

$$(1\ 3\ 4)(2\ 5) \circ (1\ 4\ 3)(2\ 5) = e = (1\ 4\ 3)(2\ 5) \circ (1\ 3\ 4)(2\ 5).$$

Exercise B89

Write down the inverse of each of the following permutations of $\{1, 2, 3, 4, 5, 6, 7, 8\}$.

(a) $(1\ 6\ 4\ 2\ 5\ 8\ 3\ 7)$ (b) $(1\ 5\ 4\ 7)(2\ 6\ 8)$ (c) $(1\ 8)(2\ 7)(3\ 5)$

Exercise B90

Let f and g be the following permutations of $\{1, 2, 3, 4, 5, 6\}$:

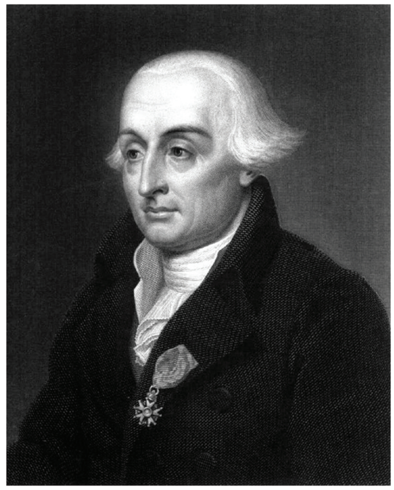
$$f = (1\ 2\ 6\ 4\ 5), \quad g = (1\ 3\ 6)(2\ 5\ 4).$$

(a) Write down the following permutations in cycle form.

(i) $g \circ f$ (ii) f^{-1} (iii) g^{-1} (iv) $(g \circ f)^{-1}$

(b) Verify that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Permutations have been an object of study for many centuries. For example, they appear in India as early as 1150 in the work of Bhāskara II (1114–1185). However, from the point of view of group theory, the starting point for their study is a paper by Joseph-Louis Lagrange (1736–1813) of 1770/71 on the theory of algebraic equations.



Joseph-Louis Lagrange

2 Permutation groups

We now go on to look at some groups whose elements are permutations, and some properties of the permutations in these groups.

2.1 The symmetric group S_n

We denote the set of all permutations of the set $\{1, 2, 3, \ldots, n\}$ by S_n. The set S_n forms a group under function composition, as stated and proved below.

Theorem B52

The set S_n of all permutations of the set $\{1, 2, 3, \ldots, n\}$ is a group under function composition.

Proof We check that the four group axioms hold. (The group axioms were given in Subsection 3.1 of Unit B1.)

Let $S = \{1, 2, 3, \ldots, n\}$.

G1 Closure

We have seen that the composite $g \circ f$ of any two permutations f and g of S is itself a permutation of S. That is, for all f, $g \in S_n$, we have $g \circ f \in S_n$.

G2 Associativity

Function composition is an associative binary operation.

G3 Identity

The identity permutation e, which fixes every symbol of S, is an identity element in S_n.

G4 Inverses

We have seen that each permutation f of the set S has an inverse permutation f^{-1}, which is also a permutation of S. (The permutations f and f^{-1} satisfy the equation $f \circ f^{-1} = e = f^{-1} \circ f$ by the definition of an inverse function: see the discussion at the end of Section 3.4 in Unit A1 *Sets, functions and vectors*.) That is, each permutation $f \in S_n$ has an inverse $f^{-1} \in S_n$.

Hence S_n is a group. ■

In Unit B2 you met the convention that if the binary operation of a group $(G, \circ)$ is clear from the context, then we often refer to the group simply as the group G, rather than the group $(G, \circ)$. We use this convention for the group $(S_n, \circ)$: we usually refer to it simply as the group S_n, with the understanding that the binary operation is function composition.

Definition

The group S_n of all permutations of the set $\{1, 2, 3, \ldots, n\}$ is called the **symmetric group of degree n**.

Although the symmetric group S_n is defined to be the group of all permutations of the set $\{1, 2, 3, \ldots, n\}$, notice that the actual symbols being permuted do not matter in the proof of Theorem B52 above, so the proof shows that the set of permutations of *any* set of n symbols forms a group under function composition. Sometimes it is useful to take the set of n symbols being permuted to be a set other than the usual set $\{1, 2, 3, \ldots, n\}$, as you will see later.

William Burnside

The term *symmetric group* first appeared in English in 1897 in *Theory of Groups of Finite Order*, the classic work of William Burnside (1852–1927) and the first treatise on group theory in English. Burnside, who began his career at the University of Cambridge, was professor of mathematics at the Royal Naval College at Greenwich from 1885 until 1919. He was one of the leading group theorists of his generation.

Be careful not to confuse a *symmetric* group with a *symmetry* group: a symmetry group is a group of symmetries of a figure.

Also, be careful not to confuse the *degree* and the *order* of a symmetric group. Its degree is the number of symbols that its elements permute, whereas, just as for any group, its **order** is the number of elements that it has. In the next exercise you are asked to find the orders of the symmetric groups S_3 and S_4.

Exercise B91

(a) Write down all the elements of the group S_3 in two-line form and also in cycle form. What is the order of the group S_3?

(b) What is the order of the group S_4?

Hint: Do not attempt to write down all the elements of S_4. Instead, try to count how many different ways there are to complete the bottom row of the two-line form of a permutation of the set $\{1, 2, 3, 4\}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}.$$

The solution to Exercise B91 can be generalised to prove the theorem below. Remember that for any positive integer n, we write

$$n! = n \times (n-1) \times \cdots \times 2 \times 1.$$

This number is called the **factorial** of n. The notation $n!$ is read as 'n factorial' or 'factorial n'.

Theorem B53

The symmetric group S_n has order $n!$.

Proof We count how many different ways there are to complete the bottom row of the two-line form of a permutation of the set $\{1, 2, 3, \ldots, n\}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ & & & & & \end{pmatrix}.$$

There are n choices for the symbol to be placed in the first position in the bottom row.

Once we have chosen this symbol, there are only $n-1$ symbols still to be placed, so there are $n-1$ choices for the symbol to be placed in the second position.

Once we have chosen the first two symbols, there are only $n-2$ symbols still to be placed, so there are $n-2$ choices for the symbol to be placed in the third position.

We continue in this way, until, finally, there are 2 choices for the symbol to be placed in the $(n-1)$th position, and then just 1 choice for the symbol to be placed in the nth position.

The total number of ways to fill in the bottom row is therefore

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!.$$

That is, the group S_n has order $n!$. ■

The order of the group S_n grows very quickly as n increases. For example,

$$\begin{aligned}
|S_3| &= 3! = 6,\\
|S_4| &= 4! = 24,\\
|S_5| &= 5! = 120,\\
|S_6| &= 6! = 720,\\
|S_7| &= 7! = 5040,\\
|S_8| &= 8! = 40\,320.
\end{aligned}$$

(Remember that the order of a group G is denoted by $|G|$.)

Even for quite small values of n, the group S_n has many subgroups.

Definition

A **permutation group** (or **group of permutations**) is a subgroup of the group S_n, for some positive integer n.

For example, the subset

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

of the group S_4 is a permutation group, since it is a subgroup of S_4, as you will see in Subsection 2.4.

We will find more subgroups of symmetric groups in the next two subsections, and we will find all the subgroups of the particular symmetric group S_4 in Section 5.

2.2 Cycle structure

In this subsection we look at the different possible structures of the cycle form of a permutation.

The simplest type of structure is a single cycle, as defined below.

Definitions

A permutation whose cycle form consists of a single cycle permuting r symbols (with all other symbols fixed) is called an ***r*-cycle** or a **cycle of length *r***.

A 2-cycle is also called a **transposition**.

For example, in S_5,

the permutation $(1\ 5\ 2\ 4\ 3)$ is a 5-cycle

the permutation $(1\ 2\ 5\ 3)$ is a 4-cycle

the permutation $(2\ 4\ 5)$ is a 3-cycle

the permutations $(1\ 5)$ and $(2\ 3)$ are transpositions.

The following two permutations in S_5 have a cycle form that consists of more than one cycle:

the permutation $(1\ 2\ 5)(3\ 4)$ consists of a 2-cycle and a 3-cycle

the permutation $(1\ 3)(2\ 4\ 5)$ also consists of a 2-cycle and a 3-cycle.

We say that these two permutations have the *same cycle structure* in S_5.

Definition

Two permutations in S_n have the **same cycle structure** if their cycle forms contain the same number of disjoint r-cycles for each natural number r.

For example, in S_8, the permutations

$$(1\ 2\ 4)(3\ 8)(5\ 6) \quad \text{and} \quad (1\ 7)(2\ 8\ 3)(4\ 5)$$

have the same cycle structure, since each consists of a 3-cycle, two 2-cycles and a 1-cycle (the 1-cycle is for the fixed symbol that does not appear in the cycle form). On the other hand, the permutations

$$(2\ 6\ 3)(4\ 8) \quad \text{and} \quad (1\ 8)(2\ 3)(4\ 6\ 7)$$

in S_8 have different cycle structures, since, for example, the first permutation has just one 2-cycle whereas the second has two.

The concept of cycle structure is useful when we want to determine all the permutations in S_n in cycle form for a particular value of n. We can start by working out which cycle structures are possible.

Worked Exercise B36

Write down all the possible cycle structures in S_3, and list all the permutations in S_3 with each cycle structure.

Solution

There are three possible cycle structures in S_3. These are given in the table below, together with the corresponding elements of S_3.

Cycle structure	Elements of S_3	Description
e	e	identity
$(-\ -)$	$(1\ 2),\ (1\ 3),\ (2\ 3)$	transpositions
$(-\ -\ -)$	$(1\ 2\ 3),\ (1\ 3\ 2)$	3-cycles

In Worked Exercise B36 we could have written the cycle structure of the identity permutation e as $(-)(-)(-)$, but it is more convenient just to write e.

Exercise B92

Write down all the possible cycle structures in S_4, and give one permutation with each cycle structure.

Exercise B93

Find as many cycle structures as you can in S_5, and write down one permutation with each cycle structure you find.

2.3 Order of a permutation

In Unit B2 you saw that the **order** of an element x of a group $(G, \circ)$ is the smallest positive integer n such that $x^n = e$. In this subsection we will look at how we can determine the order of a permutation in S_n.

Let us start by investigating the order of a permutation that consists of a single cycle. Consider, for example, the following 5-cycle in S_6:

$$f = (1\ 3\ 2\ 4\ 6).$$

We can find the order of f by evaluating $f^2, f^3, \ldots,$ until we reach the identity permutation e. (Remember that f^2 denotes $f \circ f$, and f^3 denotes $f \circ f \circ f$, and so on.) These powers of f can be found by using the usual method for composing permutations, but there is a quicker way: they can be read from the cycle form of f.

For example, the permutation f^2 is obtained by applying f twice to each symbol, which amounts to mapping each symbol to the symbol two places around the cycle, as shown in Figure 5(a).

Therefore

$$f^2 = (1\ 2\ 6\ 3\ 4).$$

(The symbol 5 is fixed by f and by any power of f.)

Similarly, f^3 maps each symbol to the symbol three places around the cycle, as shown in Figure 5(b).

Therefore

$$f^3 = (1\ 4\ 3\ 6\ 2).$$

Applying f four times maps each symbol to the symbol four places around the cycle (or, equivalently, one place backwards), as shown in Figure 5(c).

Therefore

$$f^4 = (1\ 6\ 4\ 2\ 3).$$

Applying f five times maps each symbol to the symbol five places around the cycle; that is, f^5 maps each symbol to itself, so

$$f^5 = e.$$

Hence f has order 5.

In general, for any cycle in any symmetric group S_n, we have the following result.

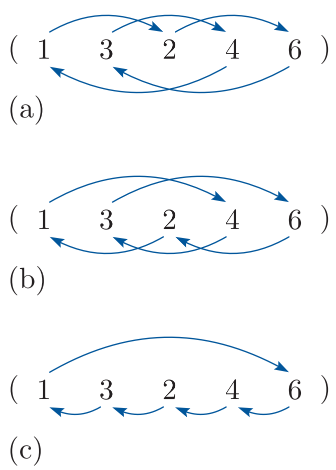


Figure 5 Mapping each symbol round a cycle (a) by two places (b) by three places (c) by four places

> **Theorem B54**
>
> An r-cycle has order r.

Proof Consider an r-cycle $f = (a_1\ a_2\ \ldots\ a_r)$. To prove that f has order r, we need to show that $f^r = e$ and also that $f^k \neq e$ for any positive integer $k < r$.

The permutation f^r (r applications of f) takes each symbol r places around the cycle; that is, back to itself. Thus f^r fixes each symbol, so $f^r = e$.

Also, for each positive integer $k < r$, the kth power of f takes each symbol k places around the cycle to a *different* symbol. Thus $f^k \neq e$.

It follows that the order of f is r. ■

Exercise B94

Verify Theorem B54 when f is the 6-cycle $(1\ 6\ 3\ 7\ 5\ 2)$ in S_7, by finding powers f^k of f for $k = 1, 2, 3 \ldots$ until you reach the identity permutation.

Now let us look at the question of how to determine the order of a permutation that consists of more than one disjoint cycle. Consider, for example, the following permutation f in S_9:

$$f = (1\ 2)(3\ 4\ 5\ 6)(7\ 8\ 9).$$

Since, for any positive integer k, the kth power f^k of f moves each symbol k places around the cycle of f in which it lies, we can deduce which symbols are fixed by the various powers of f, as follows:

1 and 2 are fixed by the 2nd, 4th, 6th, 8th, 10th, 12th, ... powers of f
3, 4, 5 and 6 are fixed by the 4th, 8th, 12th, ... powers of f
7, 8 and 9 are fixed by the 3rd, 6th, 9th, 12th, ... powers of f.

The smallest positive power of f that fixes all nine symbols is the 12th power, so f has order 12.

The answer 12 here is the *least common multiple* of the lengths 2, 3 and 4 of the cycles of f. Remember that the **least common multiple** of a set of non-zero integers is the smallest positive integer that is divisible by each number in the set.

The order of any permutation can be worked out in a similar way. So we have the following general result.

Theorem B55

The order of a permutation is the least common multiple of the lengths of its cycles.

Worked Exercise B37

Write down the order of the permutation

$$(1\ 4\ 8\ 5\ 6\ 9)(2\ 3\ 7).$$

Solution

The cycle lengths are 6 and 3, and the least common multiple of 6 and 3 is 6.

The permutation has order 6.

Exercise B95

Write down the order of each of the following permutations.

(a) $(3\ 5\ 4\ 9)(1\ 6)(2\ 7)$ (b) $(1\ 5\ 9)(2\ 8\ 3\ 7\ 4)$

(c) $(1\ 2)(3\ 9)(4\ 8)(5\ 6\ 7)$ (d) $(1\ 5\ 9)(2\ 4\ 6)$

As you saw in Unit B2, an element f of order n in a group G generates a cyclic subgroup $\langle f \rangle$ of order n, given by

$$\langle f \rangle = \{e, f, f^2, \ldots, f^{n-1}\}.$$

Worked Exercise B38

Find the elements of the cyclic subgroup $\langle (1\ 2\ 3) \rangle$ of S_4.

Solution

The permutation $(1\ 2\ 3)$ has order 3, so

$$\begin{aligned}\langle (1\ 2\ 3) \rangle &= \{e,\ (1\ 2\ 3),\ (1\ 2\ 3)^2\} \\ &= \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}.\end{aligned}$$

Exercise B96

Find the elements of each of the following cyclic subgroups of S_5.

(a) $\langle (1\ 5\ 2\ 3) \rangle$ (b) $\langle (1\ 4\ 2)(3\ 5) \rangle$

Exercise B97

Show that the set $S = \{e, (1\ 5\ 6), (1\ 6\ 5)\}$ is a subgroup of S_6.

2.4 Representing symmetries as permutations

In Unit B1 you saw that the symmetries of any figure F in $\mathbb{R}^2$ or $\mathbb{R}^3$ form a group under function composition, called the *symmetry group* of F and denoted by $S(F)$. You saw that if F is a polygon or polyhedron then by labelling its vertex locations we can represent its symmetries as two-line symbols.

For example, consider the square with its vertex locations labelled with the symbols 1, 2, 3 and 4 in the usual way, as shown in Figure 6. With this labelling we can represent the symmetries a and s, for instance, of the square by

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \text{and} \quad s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

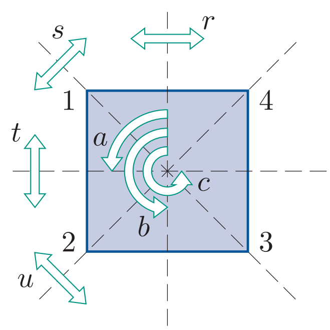


Figure 6 $S(\square)$

Since the two-line symbols that represent the symmetries of the square are permutations of the set $\{1, 2, 3, 4\}$ in two-line form, they are elements of the symmetric group S_4. So we can also write them in cycle form. For instance, for the two symmetries above we have

$$a = (1\ 2\ 3\ 4) \quad \text{and} \quad s = (2\ 4).$$

Cycle form is usually more convenient than two-line symbols for representing the symmetries of a figure. For example, the cycle forms above for the symmetries a and s of the square make it obvious that a maps the four vertices of the square round in a cycle, and that s interchanges the vertices at locations 2 and 4 and fixes the vertices at locations 1 and 3. So we will use cycle form rather than two-line symbols to represent elements of symmetry groups from now on.

When we want to write down the cycle form of a symmetry of a figure we can do so directly, rather than first writing it as a two-line symbol and then converting it. For example, we can see from Figure 6 that the symmetry r of the square interchanges the vertices at locations 1 and 4 and also interchanges the vertices at locations 2 and 3, so

$$r = (1\ 4)(2\ 3).$$

All the symmetries of the square are listed in cycle form in Table 1, along with their orders. The orders of these symmetries were found in Unit B1, but notice that we can also find them directly from the cycle forms using Theorem B55. For example, the symmetry r consists of two 2-cycles, so its order is the least common multiple of 2 and 2, which is 2.

Table 1 The symmetries in $S(\square)$ in cycle form

	Symmetry	Order
Rotations	e	1
	$a = (1\ 2\ 3\ 4)$	4
	$b = (1\ 3)(2\ 4)$	2
	$c = (1\ 4\ 3\ 2)$	4
Reflections	$r = (1\ 4)(2\ 3)$	2
	$s = (2\ 4)$	2
	$t = (1\ 2)(3\ 4)$	2
	$u = (1\ 3)$	2

As you saw in Unit B1 (with two-line symbols), we can compose symmetries of the square by composing the permutations that represent them. Since the symmetries of the square *form a group*, it follows that the eight permutations in Table 1 form a subgroup of the group S_4. So $S(\square)$ can be regarded as a subgroup of S_4.

Similarly, if we label the vertex locations of the equilateral triangle with the symbols 1, 2 and 3, then the permutations of these symbols that represent the symmetries of the triangle form a subgroup of the group S_3. So $S(\triangle)$ can be regarded as a subgroup of S_3. (In fact, since also $S(\triangle)$ and S_3 have the same order, $S(\triangle)$ can be regarded as being equal to S_3.)

The same is true in general: if a figure has n vertices and we label the locations of these vertices with the symbols $1, 2, \ldots, n$, then the permutations of these symbols that represent the symmetries of the figure form a subgroup of the group S_n.

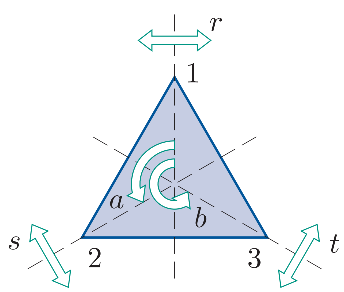


Figure 7 $S(\triangle)$

Exercise B98

Write down in cycle form all the symmetries of the equilateral triangle, when the triangle is labelled in the usual way, as shown in Figure 7. State the order of each symmetry.

Exercise B99

Write down in cycle form all the symmetries of the rectangle, when the rectangle is labelled in the usual way, as shown in Figure 8. State the order of each symmetry.

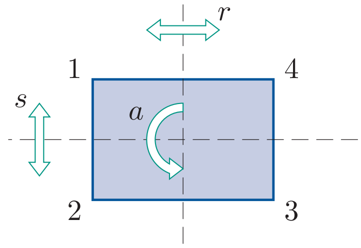
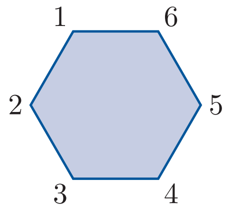


Figure 8 $S(\square)$

Exercise B100

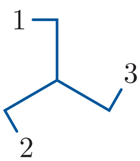
Write down in cycle form all the symmetries of the labelled regular hexagon shown below, and state the order of each symmetry. You do not need to use letters to denote the symmetries.



We can often use permutations to represent the symmetries of a plane figure even if it is not a polygon, as illustrated by the following exercise.

Exercise B101

Write down the permutations in S_3 that represent the symmetries of the following labelled figure.

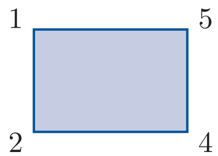


Now consider Exercise B99 again, in which the vertex locations of the rectangle were labelled with the symbols 1, 2, 3, 4 in the usual way, and the symmetries of the rectangle were represented as permutations of these symbols. These permutations form a subgroup of the symmetric group S_4. Suppose now that we introduce a fifth symbol, 5, but do not use it to label anything. Then we can regard the permutations representing the symmetries of the rectangle as permutations of the symbols 1, 2, 3, 4, 5, with all of the permutations fixing the symbol 5. So the permutations then form a subgroup of the symmetric group S_5.

In the same way, we can choose any four symbols from the five symbols 1, 2, 3, 4, 5, use them to label the vertex locations of the rectangle, and hence obtain a subgroup of the symmetric group S_5. Each permutation in this subgroup fixes the symbol not used as a label. This is illustrated in the next exercise.

Exercise B102

Find a subgroup of the symmetric group S_5 by writing down in cycle form all the symmetries of the rectangle when it is labelled as shown below.



We can use the same idea to obtain a subgroup of the symmetric group S_6. We label the vertices of the rectangle with four symbols from the set $\{1, 2, 3, 4, 5, 6\}$ and regard the other two symbols as fixed.

In general, if we label the vertex locations of a figure with some or all of the symbols from the set $\{1, 2, \ldots, n\}$, then the permutations of these symbols that represent the symmetries of the figure form a subgroup of the symmetric group S_n. Any symbols in $\{1, 2, \ldots, n\}$ that are not used to label the figure are taken to be fixed. Later in the unit we will use this idea to find some of the subgroups of the symmetric group S_4.

So far we have represented the symmetries of a figure as permutations by labelling the *vertex* locations of the figure. However, we can represent the symmetries of a figure as permutations in other ways, by labelling the locations of other features of the figure, such as its edges.

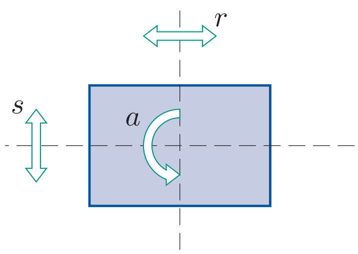
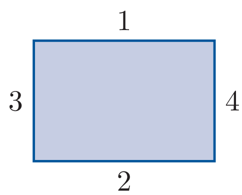


Figure 9 $S(\text{▭})$

Exercise B103

The edge locations of a rectangle are labelled 1, 2, 3 and 4 as shown below. Write down, in cycle form, the four elements of the group $S(\text{▭})$ when they are expressed as permutations of these four symbols. (The non-identity elements of $S(\text{▭})$ are shown in Figure 9.)



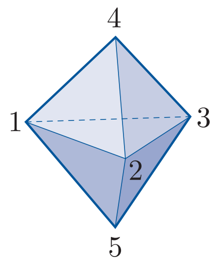
We can represent the symmetries of a figure in $\mathbb{R}^3$ by permutations in cycle form in the same way as the symmetries of a plane figure. As with plane figures, the symmetries of a figure in $\mathbb{R}^3$ form a group, so when they are represented by permutations they form a subgroup of a symmetric group.

The next worked exercise involves the symmetries of the **double tetrahedron**, which is the solid formed by sticking together two regular tetrahedrons of the same size, as illustrated in the worked exercise.

Remember from Unit B1 that the **direct** symmetries of a figure in $\mathbb{R}^3$ are those that can be demonstrated physically with a model of the figure; for a bounded figure these are the rotations. The symmetries that cannot be demonstrated physically with a model are the **indirect** symmetries. By Theorem B22 in Unit B1, if a figure in $\mathbb{R}^3$ has a finite number of symmetries, then either all the symmetries are direct, or half of the symmetries are direct and half are indirect. If there are indirect symmetries, then they can all be found by composing any fixed indirect symmetry with all of the direct symmetries.

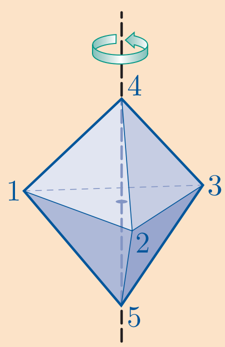
Worked Exercise B39

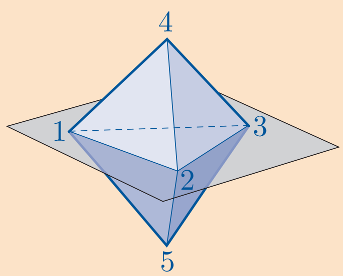
Write down the permutations in S_5 that represent the symmetries of the labelled double tetrahedron illustrated below.



Solution

First we determine how many symmetries the double tetrahedron has. There are six ways to pick it up and replace it to occupy its original space: we can rotate it about the vertical line through the vertices at locations 4 and 5, as shown on the left below, through angles of 0, $2\pi/3$ or $4\pi/3$, and we can turn it upside down and then do the same three rotations. Thus the double tetrahedron has six direct symmetries. It also has at least one indirect symmetry, such as reflection in the plane through the vertices at locations 1, 2 and 3, as shown on the right below. Since any figure with at least one indirect symmetry has the same number of indirect symmetries as direct symmetries, the double tetrahedron has 6 indirect symmetries and hence it has 12 symmetries altogether.





To find these symmetries we could first find all the direct symmetries, and then compose them all in turn with the indirect symmetry mentioned above. However, there is a slightly simpler way to proceed for this particular solid. We can observe that each symmetry of the equilateral triangle with vertices labelled 1, 2 and 3 in the middle of the solid gives a symmetry of the whole solid, and that each of these symmetries, when composed with the reflection in the plane in which this triangle lies, gives another symmetry of the whole solid.

The symmetries of the first type are represented by the permutations in the first column below. To obtain the permutations that represent the symmetries of the second type, we compose each of the symmetries in the first column with the transposition $(4\ 5)$, which represents the reflection in the horizontal plane containing the triangle. This gives the symmetries in the second column below. Since we have found 12 different symmetries, these are all the symmetries of the double tetrahedron.

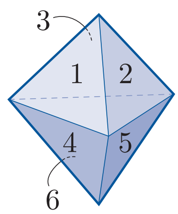
The symmetries of the double tetrahedron are represented by the following permutations in S_5.

$$\begin{array}{cc}
e & (4\ 5) \\
(1\ 2) & (1\ 2)(4\ 5) \\
(1\ 3) & (1\ 3)(4\ 5) \\
(2\ 3) & (2\ 3)(4\ 5) \\
(1\ 2\ 3) & (1\ 2\ 3)(4\ 5) \\
(1\ 3\ 2) & (1\ 3\ 2)(4\ 5)
\end{array}$$

In the next exercise you are asked to find the symmetries of the double tetrahedron when its face locations are labelled.

Exercise B104

Write down the permutations in S_6 that represent the symmetries of the double tetrahedron when its face locations are labelled as shown below.



Hint: You can proceed as in Worked Exercise B39, though finding the composites involves a little more work.

In Worked Exercise B39 we represented the symmetry group of the double tetrahedron as a subgroup of S_5, by labelling the vertex locations, and then in Exercise B104 we represented the same symmetry group as a subgroup of S_6, by labelling the face locations. We could also represent the same symmetry group as a subgroup of S_9 by labelling the edge locations, as shown in Figure 10.

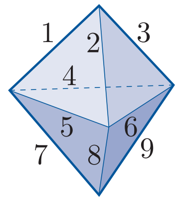


Figure 10 The double tetrahedron with its edges labelled

This illustrates that different permutation groups representing the same symmetry group may involve different numbers of symbols being permuted. The orders of these different permutation groups (that is, the number of elements that they contain) must be the same, of course.

The material in the blue box below is rather more complicated than in most of them, but you may find it interesting. Remember that the material in all the blue boxes is optional.

Permutations and bell ringing

The bells of a church ring with different pitches. Each bell is rung by pulling a rope to swing it, but there is a minimum time interval between successive strokes of the same bell, so bell ringers cannot play tunes. Instead, they often aim to ring a sequence in which each bell rings exactly once, then another such sequence with the bells in a different order, then another, and so on, until they have rung a number of such sequences, all different, in some sort of pattern. Ideally the pattern should be one that is not too hard for the bell ringers to remember. The order of the sequences in the pattern must be such that each bell changes by at most one place from each sequence to the next, to avoid the interval between successive rings of the same bell being less than the minimum possible.

For example, suppose there are three bells, A, B and C. Then there are six possible sequences of bells (since $3! = 6$), as follows:

$$ABC,\ ACB,\ BAC,\ BCA,\ CAB,\ CBA.$$

Here is a suitable order for ringing the three bells, which includes all six possible sequences; such an order is known as an *extent*. The coloured lines trace the changes in place of each bell. You can see that each bell changes by at most one place from each sequence to the next.

$A\ B\ C$
$B\ A\ C$
$B\ C\ A$
$C\ B\ A$
$C\ A\ B$
$A\ C\ B$

Church bells

Bell ringers

For larger numbers of bells it becomes harder to find an extent, but we can use group theory to help us do it.

Here is how we can think of the extent for three bells above in terms of group theory. To get from the first sequence to the second, we swap the bells in places 1 and 2; that is, we apply the transposition of places (1 2). In fact, the only permutations of places allowed from one sequence to the next in the extent are the transpositions (1 2) and (2 3), since anything else involves a bell changing by more than one place. In the extent these two transpositions are applied alternately, as shown below.

Sequence of bells	Transposition applied
A B C	
B A C	(1 2)
B C A	(2 3)
C B A	(1 2)
C A B	(2 3)
A C B	(1 2)

The second sequence of the extent is obtained from the first sequence by applying the transposition (1 2), but we can also determine how each of the other sequences is obtained *from the first sequence*, as follows.

The third sequence is obtained by applying the transposition (1 2) followed by the transposition (2 3); that is, by applying the permutation

$$(2\ 3) \circ (1\ 2) = (1\ 3\ 2).$$

Similarly, the fourth sequence is obtained by applying (1 2) followed by (2 3) followed by (1 2); that is, by applying

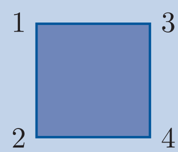
$$(1\ 2) \circ (2\ 3) \circ (1\ 2) = (1\ 3).$$

The table below shows the permutation of places obtained in this way corresponding to each sequence in the extent. The six permutations of places are all different, corresponding to the fact that the sequences they give are all different. Thus the six permutations of places are the six elements of the symmetric group S_3.

Sequence of bells	Transposition applied	Permutation from start
A B C		e
B A C	$(1\ 2)$	$(1\ 2)$
B C A	$(2\ 3)$	$(1\ 3\ 2)$
C B A	$(1\ 2)$	$(1\ 3)$
C A B	$(2\ 3)$	$(1\ 2\ 3)$
A C B	$(1\ 2)$	$(2\ 3)$

For four bells, the only permutations of places allowed from one sequence to the next are $(1\ 2)$, $(2\ 3)$, $(3\ 4)$ and $(1\ 2)(3\ 4)$. The table below shows a partial extent for four bells, in which the permutations $(2\ 3)$ and $(1\ 2)(3\ 4)$ are applied alternately. Its pattern is similar to that of the extent for three bells above, as you can see from the coloured lines. However, it includes only eight of the $4! = 24$ possible sequences of four bells. (Applying $(2\ 3)$ to the final sequence gives the first sequence again.) The corresponding eight permutations of places are in fact the elements of the group $S(\square)$, when the square is labelled as shown on the right below.

Sequence of bells	Permutation applied	Permutation from start
A B C D		e
B A D C	$(1\ 2)(3\ 4)$	$(1\ 2)(3\ 4)$
B D A C	$(2\ 3)$	$(1\ 3\ 4\ 2)$
D B C A	$(1\ 2)(3\ 4)$	$(1\ 4)$
D C B A	$(2\ 3)$	$(1\ 4)(2\ 3)$
C D A B	$(1\ 2)(3\ 4)$	$(1\ 3)(2\ 4)$
C A D B	$(2\ 3)$	$(1\ 2\ 4\ 3)$
A C B D	$(1\ 2)(3\ 4)$	$(2\ 3)$



In Book E you can see how the idea of *cosets* can be used to extend the partial extent above to give a full extent for four bells, that is, one that includes all 24 sequences.

For larger numbers of bells – churches commonly have six bells or eight bells – it would take a long time to ring a full extent: about 25 minutes for six bells, and about 24 hours for eight bells! So bell ringers usually ring partial extents. However, a full extent on eight bells was rung by a single team at Loughborough Bell Foundry in 1963, taking about 18 hours.

(Note that usually numbers are used to represent bells and letters to represent places, but in the discussion above these notations have been swapped to fit more naturally with the theory in this unit.)

3 Even and odd permutations

In this section you will see that, for any integer $n \geq 2$, the set S_n of all permutations of the set $\{1, 2, 3, \ldots, n\}$ splits naturally into two classes of permutations, known as *even* permutations and *odd* permutations. Before you can see why, you need to learn how to express every permutation in a particular way – namely as a composite of transpositions.

3.1 Expressing a permutation as a composite of transpositions

As you saw in the previous section, a **transposition** is a 2-cycle, that is, a permutation that interchanges two symbols and leaves all the others fixed. For example, in the symmetric group S_4, which consists of all permutations of the set $\{1, 2, 3, 4\}$, the transposition $(2\ 4)$ interchanges the symbols 2 and 4 and leaves the symbols 1 and 3 fixed.

In the next exercise you are asked to find some composites of transpositions. You saw how to compose permutations in Subsection 1.2. Remember that when you compose permutations (and transpositions in particular), the order of composition is important. For example,

$$(1\ 3) \circ (1\ 2) = (1\ 2\ 3),$$

whereas

$$(1\ 2) \circ (1\ 3) = (1\ 3\ 2).$$

(In contrast, the order of the cycles in the cycle form of a permutation does not matter, but this is because those cycles are *disjoint*.) Remember, too, that we compose permutations starting with the right-most permutation. For example, the composite permutation

$$(1\ 4) \circ (1\ 3) \circ (1\ 2)$$

means

$$(1\ 2) \text{ followed by } (1\ 3) \text{ followed by } (1\ 4).$$

Exercise B105

(a) Determine the following composites of transpositions in S_4.

(i) $(1\ 4) \circ (1\ 2)$ (ii) $(1\ 3) \circ (1\ 2) \circ (1\ 4)$ (iii) $(3\ 1) \circ (3\ 4) \circ (3\ 2)$

(b) Can you see a pattern in the solution to part (a)? If so, express each of the cycles $(1\ 4\ 3)$ and $(1\ 4\ 3\ 2)$ as a composite of transpositions.

The pattern discovered in the solution to Exercise B105 is generalised in the following strategy. A justification of why the strategy works is given at the end of this subsection.

Strategy B10

To express a cycle $(a_1\ a_2\ a_3\ \ldots\ a_r)$ as a composite of transpositions, do the following.

Write the transpositions

$$(a_1\ a_2),\ (a_1\ a_3),\ (a_1\ a_4),\ \ldots,\ (a_1\ a_r)$$

in reverse order and form their composite. That is,

$$(a_1\ a_2\ a_3 \ldots\ a_r) = (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \cdots \circ (a_1\ a_3) \circ (a_1\ a_2).$$

Worked Exercise B40

Express the following cycles in S_5 as composites of transpositions.

(a) $(2\ 4\ 3\ 5)$ (b) $(1\ 3\ 2\ 5\ 4)$

Solution

Use Strategy B10.

(a) $(2\ 4\ 3\ 5) = (2\ 5) \circ (2\ 3) \circ (2\ 4)$

(b) $(1\ 3\ 2\ 5\ 4) = (1\ 4) \circ (1\ 5) \circ (1\ 2) \circ (1\ 3)$

Exercise B106

Use Strategy B10 to express the following cycles in S_7 as composites of transpositions.

(a) $(1\ 5\ 2\ 7\ 3)$ (b) $(2\ 3\ 7\ 5\ 4\ 6)$ (c) $(1\ 2\ 3\ 4\ 5\ 6\ 7)$

Notice that Strategy B10 does not produce a *unique* expression for a cycle as a composite of transpositions. For instance, $(2\ 4\ 3\ 5)$ and $(4\ 3\ 5\ 2)$ are the same 4-cycle, but with a different symbol in the first position. The strategy gives the following alternative expressions as composites of transpositions:

$$\begin{aligned} (2\ 4\ 3\ 5) &= (2\ 5) \circ (2\ 3) \circ (2\ 4) \\ = (4\ 3\ 5\ 2) &= (4\ 2) \circ (4\ 5) \circ (4\ 3). \end{aligned}$$

However, for any particular cycle, the strategy always produces an expression with the same *number* of transpositions, as illustrated in the next exercise.

Exercise B107

How many transpositions do you obtain if you use Strategy B10 to express each of the following as a composite of transpositions?

(a) A 4-cycle. (b) A 5-cycle. (c) An r-cycle (for $r \geq 2$).

Although Strategy B10 is a method for expressing any *cycle* as a composite of transpositions, we can use it to express any *permutation* as a composite of transpositions, as demonstrated next.

Worked Exercise B41

Express the permutation $(1\ 9)(2\ 3\ 6\ 7)(4\ 8\ 5)$ as a composite of transpositions.

Solution

Use the fact that the permutation is equal to the composite of its disjoint cycles, and apply Strategy B10 to each of the cycles.

$$\begin{aligned} (1\ 9)(2\ 3\ 6\ 7)(4\ 8\ 5) &= (1\ 9) \circ (2\ 3\ 6\ 7) \circ (4\ 8\ 5) \\ &= (1\ 9) \circ (2\ 7) \circ (2\ 6) \circ (2\ 3) \circ (4\ 5) \circ (4\ 8). \end{aligned}$$

Thus we have the following theorem.

Theorem B56

Every permutation can be expressed as a composite of transpositions.

Proof A permutation in cycle form can be expressed as a composite of transpositions by applying Strategy B10 to each of its cycles. ∎

Exercise B108

Express each of the following permutations in S_8 as a composite of transpositions.

(a) $(1\ 8\ 3)(2\ 6\ 5\ 7)$ (b) $(1\ 7)(2\ 6\ 8)(3\ 4\ 5)$

To end this subsection, here is a proof that Strategy B10 works.

Theorem B57

If $a_1, a_2, \ldots, a_r$ are symbols (where $r \geq 2$), then the composite of transpositions

$$(a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \cdots \circ (a_1\ a_3) \circ (a_1\ a_2)$$

is equal to the cycle

$$(a_1\ a_2\ a_3 \ldots a_r).$$

Proof We can check this by finding the cycle form of the composite of transpositions in the usual way.

First we consider the symbol a_1. The first transposition $(a_1\ a_2)$ maps a_1 to a_2 and the remaining transpositions map a_2 to itself, so the composite maps a_1 to a_2.

Now we consider any symbol a_s where $2 \leq s \leq r-1$ (we consider a_r later). We see that

- each of the transpositions

  $$(a_1\ a_2),\ (a_1\ a_3),\ \ldots,\ (a_1\ a_{s-1})$$

  maps a_s to itself
- the next transposition $(a_1\ a_s)$ maps a_s to a_1
- then the next transposition $(a_1\ a_{s+1})$ maps a_1 to a_{s+1}
- and each of the remaining transpositions

  $$(a_1\ a_{s+2}),\ \ldots,\ (a_1\ a_r)$$

  maps a_{s+1} to itself.

Hence the composite maps a_s to a_{s+1}.

It remains to find the image of a_r. The symbol a_r is mapped to itself by all the transpositions except the final one $(a_1\ a_r)$, which maps a_r to a_1. Hence the composite maps a_r to a_1.

Thus the cycle form of the composite of transpositions is the cycle $(a_1\ a_2\ a_3\ \ldots\ a_r)$, as required. ■

3.2 Parity of a permutation

A permutation can be expressed as a composite of transpositions in many different ways, not all of which arise from the method that you saw in the previous subsection. The different ways do not all contain the same number of transpositions. For example, here are a few ways of expressing the 3-cycle $(1\ 2\ 3)$ in S_3 as a composite of transpositions:

$$\begin{aligned}(1\ 2\ 3) &= (1\ 3) \circ (1\ 2)\\ &= (1\ 2) \circ (2\ 3)\\ &= (2\ 3) \circ (1\ 3)\\ &= (2\ 3) \circ (1\ 2) \circ (2\ 3) \circ (1\ 2)\\ &= (1\ 2) \circ (2\ 3) \circ (3\ 1) \circ (3\ 2) \circ (2\ 1) \circ (2\ 3).\end{aligned}$$

You can check that each of these expressions is equal to $(1\ 2\ 3)$ by composing the transpositions. Notice that each of the expressions involves an *even* number of transpositions.

It turns out that if a permutation can be expressed in *one* way as a composite of an even number of transpositions, then *every* way of expressing it as a composite of transpositions involves an even number of transpositions. Similarly, if a permutation can be expressed in *one* way as a composite of an odd number of transpositions, then *every* way of expressing it as a composite of transpositions involves an odd number of transpositions. In other words, we have the following result.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

A proof of this theorem is given at the end of this section, in Subsection 3.4.

The theorem tells us that permutations can be classified into two kinds, which we call *odd* permutations and *even* permutations, as defined below.

Definitions

A permutation is **even** if it can be expressed as a composite of an even number of transpositions.

A permutation is **odd** if it can be expressed as a composite of an odd number of transpositions.

The evenness/oddness of a permutation is called its **parity**.

For example, the permutation $(1\ 2\ 3\ 4)$ in the group S_4 is odd, since

$$(1\ 2\ 3\ 4) = (1\ 4) \circ (1\ 3) \circ (1\ 2).$$

This equation shows that $(1\ 2\ 3\ 4)$ can be expressed in one way (and therefore in every way) as a composite of an odd number of transpositions.

On the other hand, the permutation $(1\ 3\ 5\ 4\ 2)$ in S_5 is even, since

$$(1\ 3\ 5\ 4\ 2) = (1\ 2) \circ (1\ 4) \circ (1\ 5) \circ (1\ 3).$$

This equation shows that $(1\ 3\ 5\ 4\ 2)$ can be expressed in one way (and therefore in every way) as a composite of an even number of transpositions.

Note that a transposition is an odd permutation, since it is a composite of one transposition, namely itself.

The identity permutation e is an even permutation, because it can be expressed as a composite of two transpositions, such as

$$e = (1\ 2) \circ (1\ 2).$$

(Alternatively, you may regard e as a composite of no transpositions; and 0 is even.)

Also, an r-cycle is a composite of $r - 1$ transpositions, as found in the solution to Exercise B107(c), so an r-cycle is an even permutation when r is odd and an odd permutation when r is even.

These facts are collected together in the following theorem.

Theorem B59

In the group S_n,

$$\text{an } r\text{-cycle is } \begin{cases} \text{an even permutation,} & \text{if } r \text{ is odd,} \\ \text{an odd permutation,} & \text{if } r \text{ is even.} \end{cases}$$

In particular, a transposition is an odd permutation and the identity permutation is an even permutation.

Exercise B109

(a) Determine whether each of the following permutations in S_6 is even or odd:

$$(1\ 2\ 5\ 3), \quad (1\ 6\ 2\ 5\ 4).$$

(b) Use the solution to Exercise B108 to classify each of the following permutations in S_8 as even or odd:

$$(1\ 8\ 3)(2\ 6\ 5\ 7), \quad (1\ 7)(2\ 6\ 8)(3\ 4\ 5).$$

(c) Determine the parity of the permutation $(1\ 8\ 2\ 7\ 6)(3\ 5\ 9\ 4)$.

Notice that if f and g are permutations in S_n, then the parity of $g \circ f$ can be deduced directly from the parities of f and g. For example, if f and g are both even, then we can replace each of the permutations f and g in $g \circ f$ by a composite of an even number of transpositions: this gives an expression for $g \circ f$ as an even number of transpositions, so $g \circ f$ is even.

In general, for any permutations f and g in S_n, we can deduce the parity of $g \circ f$ from the parities of f and g by using the fact that the addition of even and odd integers has the pattern in the table below.

$+$	even	odd
even	even	odd
odd	odd	even

Thus if f and g are both even or both odd, then $g \circ f$ is even, whereas if f and g have different parities, then $g \circ f$ is odd.

These observations enable us to find the parity of a permutation without having to write out any transpositions.

Worked Exercise B42

Determine the parity of the following permutation in S_9:

$$(1\ 2\ 3\ 4)(5\ 6)(7\ 8\ 9).$$

Solution

Use the fact that the permutation is equal to the composite of its disjoint cycles:

$$(1\ 2\ 3\ 4)(5\ 6)(7\ 8\ 9) = (1\ 2\ 3\ 4) \circ (5\ 6) \circ (7\ 8\ 9).$$

Find the parity of each cycle, using the fact that a cycle of even length is odd and a cycle of odd length is even.

$$\underbrace{(1\ 2\ 3\ 4)}_{\text{odd}} \circ \underbrace{(5\ 6)}_{\text{odd}} \circ \underbrace{(7\ 8\ 9)}_{\text{even}}$$

Deduce the parity of the composite permutation.

The parity of the permutation is

$$\text{odd} + \text{odd} + \text{even} = \text{even}.$$

In Worked Exercise B42 we worked out the parity of a composite of disjoint cycles by finding the parity of each cycle and deducing the overall parity. We can use the same method to work out the parity of any composite of permutations – it does not matter whether the cycles that form the composite are disjoint or not.

Worked Exercise B43

Determine the parity of the following composite in S_6:

$$(1\ 2\ 4)(3\ 5) \circ (1\ 3)(2\ 4\ 6\ 5) \circ (1\ 5\ 2\ 6\ 3\ 4).$$

Solution

We have

$$(1\ 2\ 4)(3\ 5) \circ (1\ 3)(2\ 4\ 6\ 5) \circ (1\ 5\ 2\ 6\ 3\ 4)$$
$$= (1\ 2\ 4) \circ (3\ 5) \circ (1\ 3) \circ (2\ 4\ 6\ 5) \circ (1\ 5\ 2\ 6\ 3\ 4).$$

The given composite is

$$\text{even} + \text{odd} + \text{odd} + \text{odd} + \text{odd} = \text{even}.$$

The ideas illustrated in Worked Exercises B42 and B43 are collected in the following general strategy.

Strategy B11

To determine the parity of a permutation, do the following.

1. Express the permutation as a composite of cycles (either disjoint or not).
2. Find the parity of each cycle, using the rule:

$$\text{an } r\text{-cycle is } \begin{cases} \text{even}, & \text{if } r \text{ is odd}, \\ \text{odd}, & \text{if } r \text{ is even}. \end{cases}$$

3. Combine the even and odd parities using the following table.

+	even	odd
even	even	odd
odd	odd	even

Exercise B110

Use Strategy B11 to determine the parity of each of the following composite permutations in S_5.

(a) $(1\ 2\ 4)(3\ 5) \circ (1\ 5\ 2)$ (b) $(1\ 2\ 4) \circ (1\ 3)(2\ 5\ 4) \circ (1\ 2\ 3\ 4)$

You may have noticed from Worked Exercise B43 and Exercise B110 that steps 2 and 3 of Strategy B11 together amount to the following rule: if the number of cycles of *even* length (that is, the number of cycles that are *odd* permutations) is

even, then the permutation is even,

odd, then the permutation is odd.

However, it is probably more helpful to remember the steps of Strategy B11 rather than this rule.

In the discussion above you saw how to deduce the parity of a composite permutation $g \circ f$ from the parity of the individual permutations f and g. We can also deduce the parity of an inverse permutation f^{-1} from the parity of the original permutation f, using the following simple result.

Theorem B60

A permutation and its inverse have the same parity.

Proof A permutation and its inverse have the same cycle structure, because we obtain the inverse by writing each cycle of the permutation in reverse order. Since it is the cycle structure alone that determines the parity of a permutation, it follows that a permutation and its inverse have the same parity. ■

An alternative way to prove Theorem B60 is to consider the parities of the permutations in the equation $f \circ f^{-1} = e$. We know that e is even, so f and f^{-1} must have the same parity, because otherwise $f \circ f^{-1}$ would be the composite of an even permutation and an odd permutation and hence would be odd.

3.3 The alternating group A_n

We denote the set of all *even* permutations of the set of symbols $\{1, 2, 3, \ldots, n\}$ by A_n. Thus A_n is a subset of S_n.

In fact, A_n is a *subgroup* of S_n, as shown below.

Theorem B61

The set A_n of all even permutations of the set $\{1, 2, 3, \ldots, n\}$ is a subgroup of the symmetric group S_n.

Proof We check that the three subgroup properties SG1, SG2 and SG3 hold. (These are given in Theorem B24 of Unit B2.)

SG1 Closure We have seen that the composite of two even permutations is an even permutation. That is, for all f, $g \in A_n$, the composite $g \circ f$ is in A_n.

SG2 Identity The identity permutation e is even, so e is in A_n.

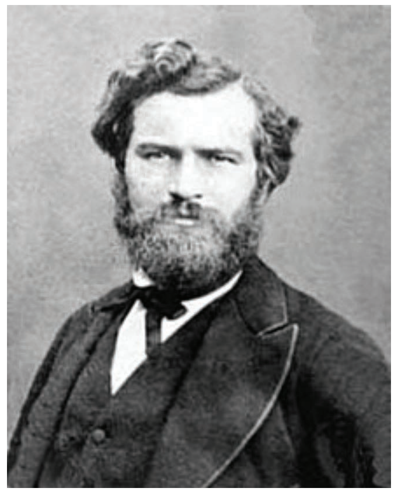
SG3 Inverses We have seen that a permutation and its inverse have the same parity. In particular, the inverse of an even permutation is itself an even permutation. That is, for each $f \in A_n$, its inverse f^{-1} is in A_n.

Thus A_n satisfies the three subgroup properties, and so is a subgroup of S_n. ■

Definition

The group A_n of all even permutations of $\{1, 2, \ldots, n\}$ is called the **alternating group of degree n**.

The term *alternating group* was introduced in 1873 by Camille Jordan (1838–1922), whose contribution to group theory has already been mentioned in Unit B2. Jordan, who studied mathematics at the École Polytechnique in Paris, trained as an engineer and continued in that profession, at least by name, until 1885. It was while working as an engineer that he did most of his mathematical research, publishing papers on a wide variety of topics ranging from topology to mechanics, as well as in group theory, the subject in which he was seen as the undisputed master for forty years.



Camille Jordan

Exercise B111

List the elements of the alternating group A_3, and hence state the order of this group. (The elements of the symmetric group S_3 were found in Worked Exercise B36.)

Now let us find the elements of the alternating group A_4. The cycle structures in the symmetric group S_4 (found in the solution to Exercise B92) are

$$e, \quad (-\,-), \quad (-\;-\;-), \quad (-\;-\;-\;-), \quad (-\,-)(-\,-).$$

Their corresponding parities are, respectively,

$$\text{even}, \quad \text{odd}, \quad \text{even}, \quad \text{odd}, \quad \text{odd} + \text{odd} = \text{even}.$$

So the possible cycle structures in A_4 are

$$e, \quad (-\;-\;-), \quad (-\,-)(-\,-).$$

The symbols in the cycles are from the set $\{1, 2, 3, 4\}$.

For the cycle structure $(-\;-\;-)$, there are four choices for the three symbols that appear in the 3-cycle, namely $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$ and $\{2, 3, 4\}$. For each of these four choices of symbols, there are two 3-cycles containing the three symbols. For example, the two 3-cycles containing the symbols 1, 2 and 3 are $(1\ 2\ 3)$ and $(1\ 3\ 2)$, because we can assume that the smallest symbol, 1, is placed first in each cycle, and there are then two different ways to place the other two symbols in the other two places.

There are three elements of A_4 with the cycle structure $(-\,-)(-\,-)$, namely $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$, because there are three choices for the symbol that is in the same transposition as the symbol 1, and the other two symbols must then be in the other transposition.

Thus the elements of A_4 are as listed in Table 2.

Table 2 The elements of the alternating group A_4

Cycle structure	Number of permutations	Elements of A_4
e	1	e
$(-\;-\;-)$	8	$(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$
$(-\,-)(-\,-)$	3	$(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$

Table 2 shows that the order of the alternating group A_4 is $1 + 8 + 3 = 12$. This is exactly half of the order of the symmetric group S_4, which is $4! = 24$. Similarly, as you saw in Exercise B111, the order of the alternating group A_3 is 3, and this is exactly half of the order of the symmetric group S_3, which is $3! = 6$. In fact, for every integer $n \geq 2$ the order of the alternating group A_n is half of the order of the symmetric group S_n. In other words, since the symmetric group S_n has order $n!$ (by Theorem B53), the alternating group A_n has order $\frac{1}{2}(n!)$. This is stated and proved below.

Theorem B62

For each integer $n \geq 2$, the alternating group A_n has order $\frac{1}{2}(n!)$.

Proof Suppose that S_n has r even permutations and s odd permutations. We will establish that $r = s$ by showing that both $r \leq s$ and $r \geq s$.

To prove that $r \leq s$, suppose that the r even permutations in S_n are $f_1, f_2, f_3, \ldots, f_r$, and consider the r permutations

$$(1\ 2) \circ f_1, \quad (1\ 2) \circ f_2, \quad (1\ 2) \circ f_3, \quad \ldots, \quad (1\ 2) \circ f_r.$$

These permutations are all odd, since each is the composite of a transposition with an even permutation.

Moreover, these r permutations are distinct, because if

$$(1\ 2) \circ f_i = (1\ 2) \circ f_j,$$

then, by the Left Cancellation Law in the group S_n,

$$f_i = f_j.$$

So we have found r odd permutations in S_n. It follows that s, the total number of odd permutations, is greater than or equal to r; that is, $r \leq s$.

A similar argument shows that if the s odd permutations in S_n are $g_1, g_2, g_3, \ldots, g_s$, then the s permutations

$$(1\ 2) \circ g_1, \quad (1\ 2) \circ g_2, \quad (1\ 2) \circ g_3, \quad \ldots, \quad (1\ 2) \circ g_s$$

are distinct even permutations in S_n, so $r \geq s$.

It follows that $r = s$, so exactly half the permutations in S_n are even.

Since S_n has order $n!$, it follows that A_n has order $\frac{1}{2}(n!)$. ■

3.4 Proof of the Parity Theorem (optional)

This subsection provides a proof of the Parity Theorem. The material in this subsection will not be assessed.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

The proof of the Parity Theorem depends on considering the number of cycles in the cycle form of a permutation, including any 1-cycles, which are usually omitted from the cycle form. We will refer to this number as the *cycle number* of the permutation. For example, the permutation

$$(1\ 4\ 3)(2\ 5)(6\ 7\ 8\ 9)$$

in S_9 has cycle number 3, and the permutation

$$(1\ 4\ 3)(2\ 5)(6\ 7)$$

in S_9 has cycle number 5, since

$$(1\ 4\ 3)(2\ 5)(6\ 7) = (1\ 4\ 3)(2\ 5)(6\ 7)(8)(9).$$

The main fact needed for the proof is as follows. Suppose that f is a permutation in S_n and $t = (a\ b)$ is a transposition in S_n. Then the cycle numbers of f and $t \circ f$ always differ by 1. If the symbols a and b lie in the same cycle in the cycle form of f, then composing with $t = (a\ b)$ cuts this cycle into two cycles; whereas if they lie in different cycles (possibly 1-cycles), then composing with $t = (a\ b)$ joins these two cycles into one cycle. This is illustrated in the following exercise.

Exercise B112

For each of the following permutations f in S_7, write down the cycle number of f. Then find $t \circ f$ in cycle form, where t is the transposition $(1\ 2)$, and write down the cycle number of $t \circ f$.

(a) $(1\ 4\ 5\ 2\ 3\ 6\ 7)$ (b) $(1\ 4\ 3)(2\ 6\ 5\ 7)$ (c) $(1\ 2\ 7\ 3)(4\ 6)$

(d) $(1\ 5\ 3)(2\ 4)(6\ 7)$

Here is a proof that the fact illustrated by Exercise B112 is true in general. (We refer to the result below as a *lemma* because it is an intermediate step in the proof of our main result, the Parity Theorem.)

Lemma B63

If f is a permutation in S_n and t is a transposition in S_n, then the cycle numbers of f and $t \circ f$ differ by 1.

Proof Let f be a permutation in S_n and let $t = (a\ b)$ be a transposition in S_n.

First suppose that the symbols a and b lie in the same cycle in the cycle form of f. Then we may write

$$f = (a\ x_1\ x_2\ \ldots\ x_r\ b\ y_1\ y_2\ \ldots\ y_s) f_1 f_2 \cdots f_m,$$

where $x_1, x_2, \ldots, x_r$ and $y_1, y_2, \ldots, y_s$ are symbols from $\{1, 2, \ldots, n\}$, and $f_1, f_2, \ldots, f_m$ are cycles in S_n that are disjoint from the cycle containing

a and b. If we use the usual method for composing permutations (starting with the symbol a), we obtain

$$\begin{aligned} t \circ f &= (a\ b) \circ (a\ x_1\ x_2\ \ldots\ x_r\ b\ y_1\ y_2\ \ldots\ y_s) f_1 f_2 \cdots f_m \\ &= (a\ x_1\ x_2\ \ldots\ x_r)(b\ y_1\ y_2\ \ldots\ y_s) f_1 f_2 \cdots f_m. \end{aligned}$$

So the cycle number of $t \circ f$ is 1 greater than that of f. This happens even if the cycle containing a and b is of the form $(a\ b\ y_1\ y_2\ \ldots\ y_s)$ or $(a\ x_1\ x_2\ \ldots\ x_r\ b)$ or simply $(a\ b)$. (Also, there may be no cycles $f_1, f_2, \ldots, f_m$ other than the cycle containing a and b in the cycle form of f, but this is of no consequence in the argument.)

Next suppose that a and b lie in different cycles of f. Then we may write

$$f = (a\ x_1\ x_2\ \ldots\ x_r)(b\ y_1\ y_2\ \ldots\ y_s) f_1 f_2 \cdots f_m,$$

where $x_1, x_2, \ldots, x_r$ and $y_1, y_2, \ldots, y_s$ are symbols from $\{1, 2, \ldots, n\}$ and $f_1, f_2, \ldots, f_m$ are cycles in S_n that are disjoint from the cycles containing a and b. We now use the usual method for composing permutations (starting with the symbol a) to obtain

$$\begin{aligned} t \circ f &= (a\ b) \circ (a\ x_1\ x_2\ \ldots\ x_r)(b\ y_1\ y_2\ \ldots\ y_s) f_1 f_2 \cdots f_m \\ &= (a\ x_1\ x_2\ \ldots\ x_r\ b\ y_1\ y_2\ \ldots\ y_s) f_1 f_2 \cdots f_m. \end{aligned}$$

So the cycle number of $t \circ f$ is 1 less than that of f. This happens even if the cycles containing a and b are of the forms $(a)(b\ y_1\ y_2\ \ldots\ y_s)$ or $(a\ x_1\ x_2\ \ldots\ x_r)(b)$ or simply $(a)(b)$. (Again, there may be no cycles $f_1, f_2, \ldots, f_m$ other than the cycles containing a and b in the cycle form of f; and again this is of no consequence in the argument.)

Thus in both cases the cycle numbers of f and $t \circ f$ differ by 1, as claimed. ■

We can now prove the Parity Theorem.

Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

Proof Let f be a permutation in S_n. Suppose that f can be expressed as a composite of r transpositions as follows:

$$f = t_r \circ t_{r-1} \circ \cdots \circ t_2 \circ t_1.$$

The cycle form of f can be found by first composing t_2 with t_1, then t_3 with the resulting permutation, and so on. There are $r-1$ such compositions to be performed and, at each of these, the cycle number either increases by 1 or decreases by 1, by Lemma B63. Suppose that it increases i times and therefore decreases $r-1-i$ times. The cycle number of t_1 is $n-1$ (since t_1 has $n-1$ cycles: it has one 2-cycle and all its other cycles are 1-cycles), so it follows that the cycle number c of f is given by

$$c = (n-1) + i - (r-1-i),$$

that is,

$$c = n + 2i - r.$$

Rearranging this equation, we obtain

$$r = n - c + 2i.$$

It follows that if $n-c$ is odd, then the number r of transpositions is odd; whereas if $n-c$ is even, then r is even. Since the numbers n and c are fixed for the permutation f (they are the number of symbols being permuted, and the cycle number of f, respectively), this proves the result. ■

Notice that the proof above gives us an alternative way of determining the parity of a permutation in cycle form: the parity is even if $n-c$ is even, and odd if $n-c$ is odd, where n is the number of symbols being permuted, and c is the cycle number of the permutation.

4 Conjugacy in S_n

In this section you will learn about the important idea of *conjugacy* in symmetric groups. In Book E *Group theory 2* you will see that this idea can be extended to all groups.

4.1 Conjugate permutations in S_n

To illustrate the idea of conjugacy we will start by considering permutations that represent the symmetries of the square. You saw in Subsection 2.4 that when the vertex locations of the square are labelled in the usual way, as shown in Figure 11, we can represent the eight symmetries of the square by the following eight permutations in cycle form.

Rotations	Reflections
e	(1 4)(2 3)
(1 2 3 4)	(2 4)
(1 3)(2 4)	(1 2)(3 4)
(1 4 3 2)	(1 3)

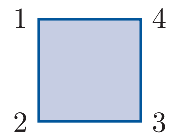


Figure 11 The square with its usual vertex labelling

Of course, the permutations that represent the symmetries of the square depend on the way that we label the vertex locations. If we relabel the vextex locations, then we obtain different permutations representing the symmetries.

For example, suppose that we use the same four labels 1, 2, 3 and 4, but relabel the vertex locations by interchanging the symbols 2 and 3, as shown in Figure 12. That is, we rearrange the labels using the transposition (2 3).

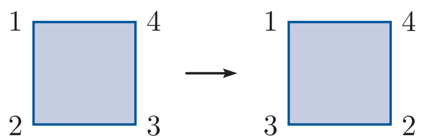


Figure 12 Relabelling the square by interchanging the labels 2 and 3

A quick way to obtain the permutations that represent the symmetries of the square with this new labelling is to take the list of permutations above and replace every occurrence of the symbol 2 with the symbol 3 and vice versa; that is, we 'rename' the symbols using the transposition (2 3). So, for example, the rotation (1 2 3 4) becomes the rotation (1 3 2 4), and the reflection (1 4)(2 3) becomes the reflection (1 4)(3 2), and so on. With the new labelling, the full list of permutations that represent the eight symmetries of the square is as follows.

Rotations	Reflections
e	(1 4)(3 2)
(1 3 2 4)	(3 4)
(1 2)(3 4)	(1 3)(2 4)
(1 4 2 3)	(1 2)

The first reflection in the list above, (1 4)(3 2), is not written in the usual way (that is, with the smallest symbol first in each cycle, and with the cycles arranged so that their smallest symbols are in increasing order). If we wish to write it in the usual way, then we obtain the following list of permutations representing the symmetries of the square.

Rotations	Reflections
e	(1 4)(2 3)
(1 3 2 4)	(3 4)
(1 2)(3 4)	(1 3)(2 4)
(1 4 2 3)	(1 2)

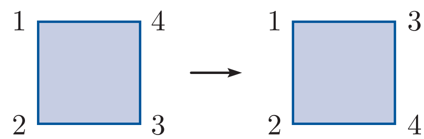
In the next exercise you are asked to write down the permutations that represent the symmetries of the square when the vertices are relabelled with the symbols 1, 2, 3 and 4 in two other ways.

Exercise B113

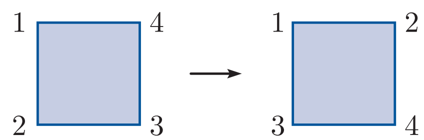
The permutations that represent the symmetries of the square when it is labelled in the usual way, as shown in Figure 11, are repeated below.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 2\ 3\ 4)$	$(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$
$(1\ 4\ 3\ 2)$	$(1\ 3)$

(a) By starting with the list of permutations above and replacing symbols as required, find the permutations that represent the symmetries of the square when it is relabelled by interchanging the labels 3 and 4, that is, by using the transposition $(3\ 4)$, as shown below.



(b) Repeat part (a) for when the vertex locations of the square are relabelled using the permutation $(2\ 3\ 4)$, as shown below.



We have now found various different ways to represent $S(\square)$ as a subgroup of the symmetric group S_4, by relabelling the vertices of the square with the symbols 1, 2, 3 and 4 in different ways. In doing so, we have found three different, but related, subgroups of S_4 (the two subgroups found in Exercise B113 are actually the same subgroup). We will return to these ideas of related subgroups in the next subsection, but first we need to look more closely at the 'symbol renaming' process that we used to obtain new representations of $S(\square)$ from the original representation. We will consider the effect of this process on a single permutation.

The process, which you carried out several times in Exercise B113, can be described as follows. We take a permutation, say x, and we rename its symbols using another permutation, say g, to obtain a third permutation, say y. We carried out this process with permutations of the set $\{1, 2, 3, 4\}$, but we can carry it out in the same way with permutations of any set of symbols.

You might expect that when this process is carried out there will be some sort of algebraic relationship between the permutations x, g and y, and indeed there is. We will now work out what it is.

Let us look at an example of the process being carried out with permutations of the set of symbols $\{1, 2, 3, 4, 5\}$; that is, permutations in S_5. Suppose that we start with the permutation $x = (1\ 2\ 5)(3\ 4)$ and rename its symbols using the permutation $g = (1\ 3\ 5\ 4)$, as illustrated below:

$$\begin{array}{rl} & x = (1\ 2\ 5)(3\ 4) \\ g\downarrow & \quad\ \ \downarrow\downarrow\downarrow\ \downarrow\downarrow \\ & y = (3\ 2\ 4)(5\ 1) \end{array} \qquad \text{where } g = (1\ 3\ 5\ 4). \tag{1}$$

That is, we replace the symbol 1 in x by the image of 1 under g, which is 3, and we replace the symbol 2 in x by the image of 2 under g, which is 2, and so on. The result is the permutation $y = (3\ 2\ 4)(5\ 1)$, as shown above. (Of course, after we have carried out these manipulations we could rewrite y in the usual way as $(1\ 5)(2\ 4\ 3)$, if we wished.)

To investigate the relationship between x, g and y, let us choose any symbol, say 4, and find the image of this symbol under the permutation y that results from the renaming. One way to find the image of 4 is simply to use the cycle form of y that was found above. This tells us that the image of 4 is 3, as illustrated below:

$$4 \xrightarrow{y} 3.$$

However, another way to find the image of 4 under y is to use the fact that y is just the permutation x with the symbols renamed, and use the cycle form of x to find the image. We proceed as follows. We first find the symbol that was renamed as 4. To do this, we need to go backwards along the arrow that points to the symbol 4 in diagram (1) above. That is, we need to find the image of 4 under the permutation g^{-1}. This gives the symbol 5. Then we use the cycle form of x to find the image of 5 under x. This gives 1. Finally, we find the symbol that is the new name of the symbol 1. That is, we find the image of 1 under the permutation g. This gives 3. So the image of 4 is 3. This process can be illustrated as follows.

$$\begin{tikzcd} 5 \arrow[r, "x"] & 1 \arrow[d, "g"] \\ 4 \arrow[u, "g^{-1}"] & 3 \end{tikzcd}$$

As expected, this process gives the same final image, 3. Thus the effect of applying the permutation y to the symbol 4 is the same as the effect of applying the permutation g^{-1}, then the permutation x, then the permutation g, to the symbol 4. That is, the two permutations y and $g \circ x \circ g^{-1}$ have the same effect on the symbol 4. There is nothing special about the symbol 4 here, of course: the same will be true for any symbol in the set $\{1, 2, 3, 4, 5\}$. In other words, we can say that the two permutations y and $g \circ x \circ g^{-1}$ are equal.

$$\begin{array}{c} x \\ g\downarrow \\ y \end{array} \qquad \begin{tikzcd} i \arrow[r, "x"] & j \arrow[d, "g"] \\ g(i) \arrow[u, "g^{-1}"] \arrow[r, "y"] & g(j) \end{tikzcd}$$

Figure 13 The effect of using a permutation g to rename the symbols in a permutation x to obtain a permutation y

The ideas above hold whenever we use a permutation g to rename the symbols in a permutation x to obtain another permutation y, as illustrated in Figure 13. In the figure, the symbol i is mapped to the symbol j by the permutation x, and the effect of the renaming is that the symbol $g(i)$ is mapped to the symbol $g(j)$ by the permutation y. By following the arrows in the figure, you can see that $g(i)$ is also mapped to $g(j)$ by the permutation $g \circ x \circ g^{-1}$. So, since $g(i)$ can be any symbol, the algebraic relationship between the three permutations x, g and y is

$$y = g \circ x \circ g^{-1}.$$

You may find this relationship rather surprising at first, but the next exercise should help to convince you that it is correct.

Exercise B114

This exercise is about permutations in S_5. Let $x = (1\ 2\ 3\ 5)$.

(a) Let $g = (1\ 4)(2\ 5\ 3)$. Calculate $g \circ x \circ g^{-1}$ by finding g^{-1} and composing the three permutations. Compare your answer with the permutation obtained by using g to rename the symbols in x.

(b) Repeat part (a) for $g = (1\ 3\ 4\ 2\ 5)$.

Because of the algebraic relationship found above, we make the following definition.

Definitions

The permutation y is a **conjugate** of the permutation x in S_n if there is a permutation g in S_n such that

$$y = g \circ x \circ g^{-1}.$$

We say that:

- g **conjugates** x to y
- y is the **conjugate** of x by g
- g is a **conjugating permutation**.

Notice that the equation

$$y = g \circ x \circ g^{-1}$$

in the definition above can be rearranged as

$$g^{-1} \circ y \circ g = x$$

(by composing both sides of the original equation on the left by g^{-1} and on the right by g). The rearranged equation can be written as

$$x = g^{-1} \circ y \circ (g^{-1})^{-1}.$$

Thus if g conjugates x to y, then g^{-1} conjugates y to x. This makes sense, because if renaming the symbols in x using g gives y, then of course renaming the symbols in y using g^{-1} gives x. So if y is a conjugate of x, then x is a conjugate of y, and we say that x and y are **conjugates**, or **conjugate permutations**.

Since renaming the symbols in a permutation does not change its cycle structure, conjugate permutations always have the same cycle structure.

In fact, it is also true that any two permutations with the same cycle structure are conjugate permutations. This is because, given any two permutations x and y with the same cycle structure, we can always find a permutation g that conjugates x to y, as demonstrated in the next worked exercise.

Worked Exercise B44

Let $x = (1\ 2\ 4)(3\ 5)$ and $y = (1\ 4)(2\ 5\ 3)$ in S_5.

(a) Find a permutation g in S_5 that conjugates x to y.

(b) Find two more permutations g in S_5 that conjugate x to y.

Solution

(a) Write the cycle form of y underneath the cycle form of x, matching up cycles of the same length. Include any 1-cycles in the cycle forms if there are any – here there are none.

We can write

$$\begin{array}{rl} x = & (1\ 2\ 4)(3\ 5) \\ g\downarrow & \ \ \downarrow\ \downarrow\ \downarrow\ \ \ \downarrow\ \downarrow \\ y = & (2\ 5\ 3)(1\ 4). \end{array}$$

This diagram is essentially the two-line form of a suitable conjugating permutation g. Write this permutation g in cycle form (using Strategy B7).

A conjugating permutation g is

$$g = (1\ 2\ 5\ 4\ 3).$$

(b) There are several alternative ways to match up the cycles in x and y, because the 3-cycle $(2\ 5\ 3)$ in y can alternatively be written as $(3\ 2\ 5)$ or $(5\ 3\ 2)$, and the 2-cycle $(1\ 4)$ in y can alternatively be written as $(4\ 1)$.

Another conjugating permutation g is given by

$$\begin{array}{rl} x = & (1\ 2\ 4)(3\ 5) \\ g\downarrow & \ \ \downarrow\ \downarrow\ \downarrow\ \ \ \downarrow\ \downarrow \\ y = & (3\ 2\ 5)(1\ 4). \end{array}$$

This gives $g = (1\ 3)(4\ 5)$.

A third conjugating permutation g is given by

$$\begin{array}{rl} & x = (1\ 2\ 4)(3\ 5) \\ g\downarrow & \quad\ \ \downarrow\downarrow\downarrow\ \ \downarrow\downarrow \\ & y = (5\ 3\ 2)(4\ 1). \end{array}$$

This gives $g = (1\ 5)(2\ 3\ 4)$.

Exercise B115

For the permutations x and y given in Worked Exercise B44, find three more permutations g in S_5 that conjugate x to y.

Here is a summary of the strategy used in Worked Exercise B44.

Strategy B12

To find a permutation g such that $y = g \circ x \circ g^{-1}$, where x and y are permutations with the same cycle structure, do the following.

Use the fact that g renames x to y, as follows.

1. Match up the cycles of x and y (including 1-cycles) so that cycles of equal lengths correspond.

$$\begin{array}{rl} & x = (*\ *\ \cdots\ *)(*\ *\ \cdots\ *)\cdots(*)(*) \\ g\downarrow & \quad\ \ \downarrow\ \downarrow\ \cdots\ \downarrow\ \ \downarrow\ \downarrow\ \cdots\ \downarrow\ \cdots\ \downarrow\ \ \downarrow \\ & y = (*\ *\ \cdots\ *)(*\ *\ \cdots\ *)\cdots(*)(*) \end{array}$$

2. Read off the two-line form of the renaming permutation g from this diagram. Usually, write g in cycle form.

Worked Exercise B44 and Exercise B115 illustrate the fact that if two permutations x and y are conjugate, then there can be many different permutations g that conjugate x to y.

You have now seen that if two permutations x and y have the same cycle structure, then it is always possible to find a permutation g that conjugates x to y, and hence x and y are conjugate. As mentioned earlier, it is also true that if two permutations are conjugate, then they have the same cycle structure (since renaming the symbols in a permutation does not change its cycle structure). Thus the following theorem holds.

Theorem B64

Two permutations in the symmetric group S_n are conjugate in S_n if and only if they have the same cycle structure.

Exercise B116

(a) Find all permutations g in S_5 such that

$$g \circ (1\ 2\ 3\ 4) \circ g^{-1} = (1\ 5\ 2\ 3).$$

(b) Find all permutations g in S_4 such that

$$g \circ (1\ 2)(3\ 4) \circ g^{-1} = (1\ 2)(3\ 4).$$

4.2 Conjugate subgroups in S_n

In this subsection we will return to looking at what happens when we use a permutation to rename the symbols in not just a single permutation, but in every permutation in a subgroup.

For example, consider again the subgroup of S_4 obtained by labelling the vertex locations of the square in the usual way, as shown in Figure 14. With this labelling, the set of symmetries of the square is represented by the following set of permutations in S_4.

$$\{e,\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2),\\ (1\ 4)(2\ 3),\ (2\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)\}$$

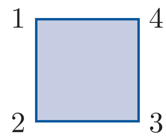


Figure 14 The square with its usual vertex labelling

This set is a subgroup of S_4, because it is a subset of S_4 and its elements represent all the symmetries of a figure.

At the start of the previous subsection we renamed the symbols in every permutation in this subgroup using the permutation $g = (2\ 3)$, which corresponds to relabelling the square as shown in Figure 15. We obtained the following set of permutations.

$$\{e,\ (1\ 3\ 2\ 4),\ (1\ 2)(3\ 4),\ (1\ 4\ 2\ 3),\\ (1\ 4)(3\ 2),\ (3\ 4),\ (1\ 3)(2\ 4),\ (1\ 2)\}$$

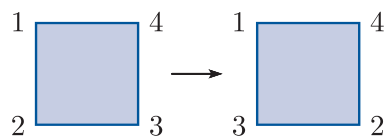


Figure 15 Relabelling the square using the permutation $g = (2\ 3)$

This set is also a subgroup of S_4, again because it is a subset of S_4 and its elements represent all the symmetries of a figure.

We will now look in general at what happens when we start with some subgroup of S_n, say H, and use a particular permutation g to rename the symbols in *all* the permutations in H.

As you saw in the previous subsection, when we rename the symbols in a single permutation x using a permutation g, the result is the conjugate permutation $g \circ x \circ g^{-1}$. In view of this, we use the following notation.

Notation

Let H be a subgroup of S_n, and let $g \in S_n$. Then we denote the set

$$\{g \circ h \circ g^{-1} : h \in H\}$$

by $g \circ H \circ g^{-1}$. That is, $g \circ H \circ g^{-1}$ is the set obtained by conjugating every element of H by the permutation g.

Thus if H is a subgroup of S_n, then $g \circ H \circ g^{-1}$ is the subset of S_n obtained by renaming the symbols in all the elements of H using g.

This definition is illustrated in the worked exercise below.

Worked Exercise B45

Let H be the cyclic subgroup of S_5 generated by the 4-cycle $(1\ 2\ 4\ 5)$; that is,

$$\begin{aligned} H &= \langle(1\ 2\ 4\ 5)\rangle \\ &= \{e, (1\ 2\ 4\ 5), (1\ 2\ 4\ 5)^2, (1\ 2\ 4\ 5)^3\} \\ &= \{e, (1\ 2\ 4\ 5), (1\ 4)(2\ 5), (1\ 5\ 4\ 2)\}. \end{aligned}$$

Find the set $g \circ H \circ g^{-1}$ where $g = (3\ 5)$.

Solution

To conjugate each element of H by $g = (3\ 5)$, we rename the symbols in each element of H using this permutation.

We have

$$g \circ H \circ g^{-1} = \{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)\}.$$

Notice that the set $g \circ H \circ g^{-1}$ found in Worked Exercise B45 is another subgroup of S_5. You can see this because it is the cyclic subgroup generated by the 4-cycle $(1\ 2\ 4\ 3)$. (This 4-cycle is obtained by using g to rename the 4-cycle $(1\ 2\ 4\ 5)$ that generates the original subgroup H.)

In the next exercise you are asked to use a particular permutation g to rename the symbols in all the permutations in another cyclic subgroup of S_5.

Exercise B117

Let H be the cyclic subgroup of S_5 generated by the 3-cycle $(1\ 3\ 5)$; that is,

$$\begin{aligned} H &= \langle(1\ 3\ 5)\rangle \\ &= \{e, (1\ 3\ 5), (1\ 3\ 5)^2\} \\ &= \{e, (1\ 3\ 5), (1\ 5\ 3)\}. \end{aligned}$$

(a) Find the set $g \circ H \circ g^{-1}$ where $g = (1\ 4)(2\ 5)$.

(b) Show that $g \circ H \circ g^{-1}$ is a subgroup of S_5.

You have now seen several examples where we took a subgroup H of a symmetric group S_n, and renamed the symbols in all its elements using a permutation g in S_n. In each case the set $g \circ H \circ g^{-1}$ that we obtained was not just a *subset* of S_n but actually a *subgroup* of S_n. In fact, this is not surprising, as all we did in each case was to rename the symbols being permuted. The general result is stated below, with a proof that uses the formal definition of the set $g \circ H \circ g^{-1}$.

Theorem B65

Let H be a subgroup of S_n, and let $g \in S_n$. Then $g \circ H \circ g^{-1}$ is also a subgroup of S_n.

Proof We check the three subgroup properties.

SG1 Closure Consider any two elements of $g \circ H \circ g^{-1}$; we can write them as $g \circ h \circ g^{-1}$ and $g \circ k \circ g^{-1}$ where $h, k \in H$. We have

$$\begin{aligned}(g \circ h \circ g^{-1}) \circ (g \circ k \circ g^{-1}) &= g \circ h \circ (g^{-1} \circ g) \circ k \circ g^{-1}\\ &= g \circ h \circ e \circ k \circ g^{-1}\\ &= g \circ h \circ k \circ g^{-1}.\end{aligned}$$

This is an element of $g \circ H \circ g^{-1}$, because $h \circ k$ is an element of H (since H is a subgroup of S_n and therefore closed under $\circ$). Thus $g \circ H \circ g^{-1}$ is closed under $\circ$.

SG2 Identity The identity permutation e is in $g \circ H \circ g^{-1}$ since $e = g \circ e \circ g^{-1}$ and $e \in H$.

SG3 Inverses Consider any element of $g \circ H \circ g^{-1}$; we can write it as $g \circ h \circ g^{-1}$ where $h \in H$. We have

$$\begin{aligned}(g \circ h \circ g^{-1})^{-1} &= (g^{-1})^{-1} \circ h^{-1} \circ g^{-1}\\ &\qquad \text{(by Proposition B14 in Unit B1, applied twice)}\\ &= g \circ h^{-1} \circ g^{-1} \quad \text{(by Proposition B13 in Unit B1).}\end{aligned}$$

This is an element of $g \circ H \circ g^{-1}$, because h^{-1} is an element of H (since H is a subgroup of S_n and therefore contains the inverse of each of its elements). Thus $g \circ H \circ g^{-1}$ contains the inverse of each of its elements.

Since $g \circ H \circ g^{-1}$ satisfies the three subgroup properties, it is a subgroup of S_n. ■

Because of Theorem B65, if H is a subgroup of S_n and g is an element of S_n, then we say that $g \circ H \circ g^{-1}$ is the **conjuate subgroup** of H by g, and that it is a **conjugate subgroup** of H in S_n.

When you are dealing with conjugate subgroups in S_n, keep in mind that if you want to find the elements of a conjugate subgroup $g \circ H \circ g^{-1}$, then you do not need to calculate composites of the form $g \circ h \circ g^{-1}$ by composing permutations. That would give you the right answer, but it would entail a lot of unnecessary calculation. Instead all you need to do is rename the symbols in each permutation h in H using g, as set out in the following strategy.

Strategy B13

To find the subgroup $g \circ H \circ g^{-1}$, given a subgroup H and an element g of S_n, do the following.

For each $h \in H$, find $g \circ h \circ g^{-1}$ by using g to 'rename' the symbols in h.

$$\begin{array}{rl} h = & (*\ *\ \cdots\ *)(*\ *\ \cdots\ *)\ \cdots\ (*\ *\ \cdots\ *) \\ g\downarrow & \ \ \downarrow\,\downarrow\,\cdots\,\downarrow\ \ \downarrow\,\downarrow\,\cdots\,\downarrow\ \ \cdots\ \ \downarrow\,\downarrow\,\cdots\,\downarrow \\ g \circ h \circ g^{-1} = & (*\ *\ \cdots\ *)(*\ *\ \cdots\ *)\ \cdots\ (*\ *\ \cdots\ *) \end{array}$$

Exercise B118

Let H be the following subgroup of S_5:

$$H = \{e, (1\ 2\ 5\ 3), (1\ 5)(2\ 3), (1\ 3\ 5\ 2)\}.$$

(H is the subgroup generated by the cycle $(1\ 2\ 5\ 3)$.)

Determine the following conjugate subgroups.

(a) $(1\ 3) \circ H \circ (1\ 3)^{-1}$ (b) $(1\ 3)(2\ 4) \circ H \circ ((1\ 3)(2\ 4))^{-1}$

Here are three more exercises that use the ideas that you have met in this subsection and the previous subsection.

Exercise B119

(a) Find all the permutations g in S_3 such that

$$g \circ (1\ 2\ 3) \circ g^{-1} = (1\ 2\ 3).$$

Show that they form a subgroup of S_3.

(b) Find all the permutations g in S_4 such that

$$g \circ (1\ 2\ 3\ 4) \circ g^{-1} = (1\ 2\ 3\ 4).$$

Show that they form a subgroup of S_4.

Exercise B120

Let $(G, \circ)$ be a group and let f be a particular element of G. Prove that the set

$$C = \{g \in G : g \circ f \circ g^{-1} = f\}$$

is a subgroup of G.

(The facts that the two sets in Exercise B119 are subgroups of S_3 and S_4, respectively, are special cases of this result.)

Exercise B121

Let H be the following subgroup of S_4:

$$H = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

(We know that this subset of S_4 is a subgroup because its elements represent the symmetries of the rectangle, as you saw in Exercise B99.)

Prove that, for each element $g \in S_4$,

$$g \circ H \circ g^{-1} = H.$$

Having now reached the end of this section, you may be wondering why we have bothered with all the theory about the algebraic relationship $y = g \circ x \circ g^{-1}$, when it seems simpler just to use the idea of renaming the symbols in a permutation! However, the relationship $y = g \circ x \circ g^{-1}$ is helpful when we want to prove results involving conjugacy, because it can be used in algebraic manipulations. Also, expressing the idea of conjugacy in terms of this algebraic relationship rather than in terms of renaming symbols allows us to apply it to groups other than the symmetric groups S_n. This is a topic that you will learn much more about in Book E.

5 Subgroups of S_4

In this section we will find subgroups of S_4, the symmetric group of degree 4, which is the group of all permutations of the set $\{1, 2, 3, 4\}$. We will start by finding all the cyclic subgroups of S_4. Then we will find some non-cyclic subgroups. By the end of the section we will have found *all* the subgroups of S_4, though we are not in a position to prove this fact at this stage. You should finish this section with some idea of the structure of S_4.

Cyclic subgroups of S_4

In seeking the subgroups of any group, it is usually easiest to start with the cyclic subgroups. Remember that each element f of a group generates a cyclic subgroup $\langle f \rangle = \{e, f, f^2, \ldots, f^{n-1}\}$ of order n, where n is the order of the element f. For example, the permutation $(1\ 2\ 3)$ in S_4, which has order 3, generates the following cyclic subgroup of S_4:

$$\begin{aligned}\langle(1\ 2\ 3)\rangle &= \{e,\ (1\ 2\ 3),\ (1\ 2\ 3)^2\}\\ &= \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}.\end{aligned}$$

It is important to remember that different elements of a group can generate the same cyclic subgroup. For example, the cyclic subgroup $\{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ of S_4 is also generated by the permutation $(1\ 3\ 2)$, since

$$\begin{aligned}\langle(1\ 3\ 2)\rangle &= \{e,\ (1\ 3\ 2),\ (1\ 3\ 2)^2\}\\ &= \{e,\ (1\ 3\ 2),\ (1\ 2\ 3)\}.\end{aligned}$$

In general, as you saw in Unit B2 *Groups and subgroups*, any element of order n in a cyclic subgroup of order n generates that subgroup.

A helpful first step towards finding all the cyclic subgroups of S_4 is to find the orders of all the elements of S_4. You saw in Theorem B55 that the order of a permutation is the least common multiple of the lengths of its cycles. Table 3 gives the five different cycle structures in S_4; you were asked to find these in Exercise B92. For each cycle structure, the table also shows the order of the elements with that cycle structure, and lists those elements.

Table 3 The cycle structures and orders of the elements of S_4

Cycle structure	Order	Elements of S_4	Description
e	1	e	identity
$(-\,-)$	2	$(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$	transpositions
$(-\,-\,-)$	3	$(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$	3-cycles
$(-\,-\,-\,-)$	4	$(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$, $(1\ 4\ 3\ 2)$	4-cycles
$(-\,-)(-\,-)$	2	$(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$	products of 2-cycles

From Table 3 we see that each element in S_4 has order 1, 2, 3 or 4, so each cyclic subgroup of S_4 has order 1, 2, 3 or 4.

Let us begin by finding the cyclic subgroups of order 3 (you are asked to find the cyclic subgroups of orders 1, 2 and 4 in the next exercise). In Subsection 4.4 of Unit B2 you saw that all cyclic groups of a particular order are isomorphic (structurally identical) to each other. They therefore contain the same number of elements of each order. In particular, each cyclic group of order 3 contains one element of order 1 (the identity) and two elements of order 3.

As shown in Table 3, the only elements of order 3 in S_4 are the 3-cycles. You saw above that the 3-cycles $(1\ 2\ 3)$ and $(1\ 3\ 2)$ each generate the subgroup $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$. The remaining six 3-cycles in S_4 'pair off' in a similar way to generate the following cyclic subgroups:

$$\langle(1\ 4\ 2)\rangle = \{e, (1\ 4\ 2), (1\ 2\ 4)\} = \langle(1\ 2\ 4)\rangle,$$
$$\langle(1\ 3\ 4)\rangle = \{e, (1\ 3\ 4), (1\ 4\ 3)\} = \langle(1\ 4\ 3)\rangle,$$
$$\langle(2\ 3\ 4)\rangle = \{e, (2\ 3\ 4), (2\ 4\ 3)\} = \langle(2\ 4\ 3)\rangle.$$

So in total there are four cyclic subgroups of order 3. In the next exercise you are asked to find all the other cyclic subgroups of S_4.

Exercise B122

Use Table 3 to help you do the following.

(a) Find all the cyclic subgroups of S_4 of orders 1, 2 and 4.

(b) Make a table showing the number of cyclic subgroups of S_4 of each possible order.

We have now found all the cyclic subgroups of S_4.

Non-cyclic subgroups of S_4

To find more subgroups of S_4 we need a method for finding non-cyclic subgroups.

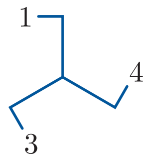
We can use a method that you met in Subsection 2.4. To find a subgroup of any symmetric group S_n, we can draw a figure, labelled at suitable locations with some or all of the symbols $1, 2, \ldots, n$, such that the symmetries of the figure can be represented by permutations of the labels. The symmetry group of the figure is then a subgroup of S_n. (Any symbols in $\{1, 2, \ldots, n\}$ that are not used to label the figure are taken to be fixed.)

This method can yield both cyclic and non-cyclic subgroups, as illustrated for subgroups of S_4 in the next worked exercise.

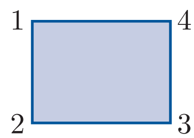
Worked Exercise B46

Each of the two figures below is labelled with some or all of the symbols 1, 2, 3 and 4.

(i)



(ii)



(a) Use each figure to find a subgroup of S_4.

(b) State whether each of the subgroups in part (a) is cyclic, justifying your answers.

Solution

(a) Using the labelling on the figures, we find that their symmetry groups can be represented by the following subgroups of S_4.

(i) $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$

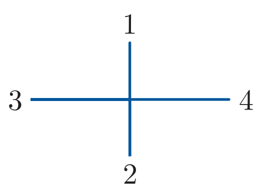
(ii) $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

(b) The subgroup in part (a)(i) is cyclic: it is generated by either of the 3-cycles that it contains. The subgroup in part (a)(ii) is non-cyclic, since it has order 4 but contains no element of order 4.

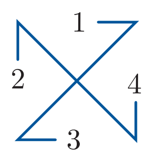
Exercise B123

(a) Use the labelled figures below to find four subgroups of S_4.

(i)

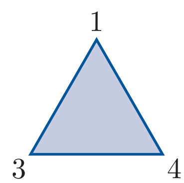


(ii)



(iii)

(iv)

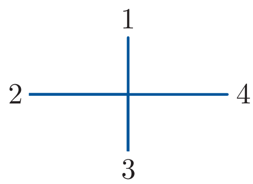


(b) Which of the subgroups in part (a) are cyclic? Justify your answers.

Once we have found a subgroup of a symmetric group that is the symmetry group of a figure, we can often find another subgroup of the same symmetric group, isomorphic to the first subgroup, by relabelling the locations on the figure. Since the new subgroup is found from the old subgroup by relabelling in this way, it is *conjugate* to the first subgroup.

Exercise B124

(a) The figure below is the same as the one in Exercise B123(a)(i), except that it has been relabelled. Use this figure to find a further subgroup of S_4.



(b) Find a third labelling of the same figure that yields a subgroup of S_4 different from the two subgroups found in part (a) and in Exercise B123(a)(i).

We have now found four different non-cyclic subgroups of S_4 of order 4, namely the one found in Worked Exercise B46, the one found in Exercise B123(a)(i) and the two found in Exercise B124. These are all isomorphic to the Klein four-group since, as you saw in Subsection 4.2 of Unit B2, the Klein four-group structure is the only possible structure for a non-cyclic group of order 4. Altogether we have now found seven subgroups of S_4 of order 4: the four non-cyclic ones, and the three cyclic ones from Exercise B122.

In the next two exercises you are asked to find subgroups of S_4 of orders 6 and 8, respectively.

Exercise B125

In Exercise B123(a)(iv) you found a subgroup of S_4 of order 6 that represents the symmetries of an equilateral triangle. By labelling the vertices of the triangle in three other ways, find three further subgroups of S_4 of order 6.

Exercise B126

(a) Use a plane figure that has a symmetry group of order 8, with appropriate labels, to find a subgroup of S_4 of order 8.

(b) By relabelling the figure in part (a) in two other ways, find two other subgroups of S_4 of order 8.

You have already met a subgroup of S_4 of order 12, namely A_4, the subgroup of even permutations in S_4. Taking this subgroup together with all the subgroups that we have found in this subsection so far, we now have all the subgroups of S_4, although a proof that there are no more subgroups is beyond the scope of this module. Table 4 gives a summary of the number of subgroups of S_4 of each order.

Table 4 The subgroups of the symmetric group S_4

Order	Number of subgroups	Description
1	1	$\{e\}$
2	9	all cyclic
3	4	all cyclic
4	7	3 cyclic; 4 Klein
6	4	all isomorphic to $S(\triangle)$
8	3	all isomorphic to $S(\square)$
12	1	A_4
24	1	S_4

Exercise B127

(a) Are all subgroups of order 2 conjugate to each other in S_4? Justify your answer.

(b) Are all subgroups of order 3 conjugate to each other in S_4? Justify your answer.

You have now seen and used two methods that give subgroups of the group S_4. A third simple way to find a subgroup of a symmetric group S_n is to find all the permutations in S_n that fix a particular symbol. For example, all the permutations in S_4 that fix the symbol 2 form a subgroup of S_4. This is because the Cayley table for these permutations looks exactly the same as the group table for the group of all permutations of the set of symbols $\{1, 3, 4\}$ (provided that we use cycle form and omit 1-cycles).

In fact, the subgroup found in Exercise B123(a)(iv) is the set of all permutations in S_4 that fix the symbol 2, and the three subgroups found in Exercise B125 are the sets of all permutations in S_4 that fix the symbols 4, 3 and 1, respectively.

More generally, we can find a subgroup of a symmetric group S_n by finding all the permutations in S_n that fix each symbol in some subset of symbols; this follows from the same argument involving Cayley tables as used above. For example, $\{e, (1\ 2)\}$ is the subgroup of S_4 that consists of all permutations in S_4 that fix each element in the subset $\{3, 4\}$; its Cayley table looks exactly the same as the group table for the group of all permutations of the set of symbols $\{1, 2\}$.

Finding subgroups of groups in general

In this section you have seen three methods for finding subgroups of S_4.

The first method, for finding cyclic subgroups, can be applied to any other group of reasonably small order. That is, you can find the cyclic subgroups of such a group by listing the elements of the group according to their orders and then systematically finding the subgroups generated by these elements.

The other two methods – namely, finding symmetry groups whose elements can be represented by permutations in S_4, and finding all permutations that fix one or more symbols – are not useful for finding subgroups of groups in general, but can be used to find subgroups of any other *symmetric group* S_n. However, it is usually difficult to find *all* the non-cyclic subgroups of a symmetric group S_n using these methods.

To find subgroups of a *symmetry group*, both cyclic and non-cyclic, you can use the methods that you saw in Subsection 1.3 of Unit B2. For example, you can modify a figure to restrict its symmetry, or find the symmetries that fix a particular vertex of the figure.

S_4 as the symmetry group of a regular tetrahedron

The symmetric group S_4 can itself be thought of as a symmetry group, namely the symmetry group of a regular tetrahedron, $S(\text{tet})$. Remember from Unit B1 that there are 24 symmetries of the tetrahedron, and if the vertex locations are labelled 1, 2, 3 and 4 as shown in Figure 16, then each such symmetry can be represented by a permutation of the symbols 1, 2, 3 and 4; that is, as an element of S_4. Moreover, since S_4 has order 24, every element of S_4 represents some symmetry of the tetrahedron. It follows that S_4 and $S(\text{tet})$ are isomorphic groups.

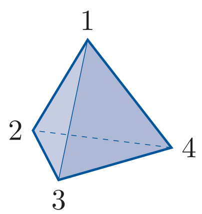


Figure 16 The regular tetrahedron

It can sometimes be enlightening to think of S_4 in this way. For example, it tells us that each of the subgroups of S_4 that we have found can be interpreted as a subgroup of $S(\text{tet})$.

For instance, with this interpretation, A_4 is the subgroup of direct symmetries of the tetrahedron. You can confirm this by checking that the twelve elements of A_4, listed in Table 2 in Subsection 3.3, are the same permutations as the twelve direct symmetries of the tetrahedron with vertex locations labelled 1, 2, 3 and 4, found in Worked Exercise B14 in Subsection 5.3 of Unit B1. (Remember that for a bounded figure in $\mathbb{R}^3$ such as the tetrahedron, the direct symmetries are the rotational symmetries.)

In the next exercise you are asked to interpret some other subgroups of S_4 as subgroups of $S(\text{tet})$. It is interesting, but rather more difficult, to do this for some of the subgroups of S_4 other than the ones considered here.

Exercise B128

Describe in words each of the following subgroups of S_4 as subgroups of $S(\text{tet})$.

(a) $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$ (b) $\{e, (3\ 4)\}$

(c) $\{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}$ (d) $\{e, (1\ 2)(3\ 4)\}$

(The subgroup in part (c) was found in Exercise B125. The other three subgroups are cyclic subgroups.)

You saw earlier, in Subsection 2.4, that the symmetric group S_3 is also isomorphic to a symmetry group, namely $S(\triangle)$, the symmetry group of the equilateral triangle.

6 Cayley's Theorem

You have seen that the symmetry groups of many figures can be represented as permutation groups. What we mean by this is that these symmetry groups are *isomorphic* (structurally identical) to permutation groups. In this section you will see that, perhaps rather surprisingly, *every* finite group is isomorphic to a permutation group.

Remember from Unit B2 that for finite groups we can define the idea of isomorphism as follows: two finite groups are **isomorphic** if there is a one-to-one and onto mapping from the first group to the second group that transforms the group table of the first group into a group table for the second group. Such a mapping is called an **isomorphism**.

For example, consider the symmetry group of the rectangle. You have seen that when the vertices of the rectangle are labelled in the usual way, as shown in Figure 17, the symmetries of the rectangle can be represented as permutations as follows:

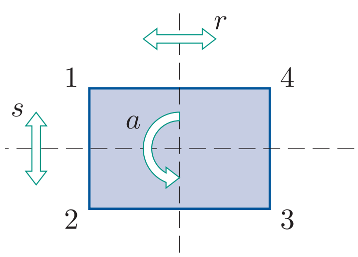


Figure 17 $S(\square)$

$$e,$$
$$a = (1\ 3)(2\ 4),$$
$$r = (1\ 4)(2\ 3),$$
$$s = (1\ 2)(3\ 4).$$

The symmetry group of the rectangle can then be represented by the permutation group $(H, \circ)$, where

$$H = \{e, (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}.$$

What we mean by this is that the two groups $(S(\square), \circ)$ and $(H, \circ)$ are isomorphic, and the mapping

$$\begin{aligned} \phi : S(\square) &\longrightarrow H \\ e &\longmapsto e \\ a &\longmapsto (1\ 3)(2\ 4) \\ r &\longmapsto (1\ 4)(2\ 3) \\ s &\longmapsto (1\ 2)(3\ 4) \end{aligned}$$

is an isomorphism. It transforms the group table of $(S(\square), \circ)$ into a group table of $(H, \circ)$, as shown below.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

$(S(\square), \circ)$

$\xrightarrow{\phi}$

$\circ$	e	$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$	$(1\ 2)(3\ 4)$
e	e	$(1\ 3)(2\ 4)$	$(1\ 4)(2\ 3)$	$(1\ 2)(3\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 3)(2\ 4)$	e	$(1\ 2)(3\ 4)$	$(1\ 4)(2\ 3)$
$(1\ 4)(2\ 3)$	$(1\ 4)(2\ 3)$	$(1\ 2)(3\ 4)$	e	$(1\ 3)(2\ 4)$
$(1\ 2)(3\ 4)$	$(1\ 2)(3\ 4)$	$(1\ 4)(2\ 3)$	$(1\ 3)(2\ 4)$	e

$(H, \circ)$

The way in which we represent the symmetry group of a figure as a permutation group is fairly intuitive: as you have seen, we label suitable locations on the figure and represent each symmetry of the figure by the corresponding permutation of the labels. It is much less obvious how we might go about representing other types of finite groups as permutation groups. However, it can be done: for example, here is how we can do it for the group $(\mathbb{Z}_6, +_6)$.

Representing the group $(\mathbb{Z}_6, +_6)$ as a permutation group

Consider the group table of $(\mathbb{Z}_6, +_6)$, as follows.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

With each element x of $\mathbb{Z}_6$ we associate the permutation p_x whose two-line form has as its first line the column headings of the group table and as its second line the row labelled x. For example, the element 2 of $\mathbb{Z}_6$ has associated permutation

$$p_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 0 & 1 \end{pmatrix}.$$

This gives us six permutations p_0, p_1, p_2, p_3, p_4, p_5, each permuting the set of symbols $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

We can write the six permutations p_0, p_1, p_2, p_3, p_4, p_5, in cycle form. For example, for the permutation p_2, given above, we have

$$p_2 = (0\ 2\ 4)(1\ 3\ 5).$$

Doing this for all six permutations we obtain

$$\begin{aligned}
p_0 &= (0)(1)(2)(3)(4)(5) = e,\\
p_1 &= (0\ 1\ 2\ 3\ 4\ 5),\\
p_2 &= (0\ 2\ 4)(1\ 3\ 5),\\
p_3 &= (0\ 3)(1\ 4)(2\ 5),\\
p_4 &= (0\ 4\ 2)(1\ 5\ 3),\\
p_5 &= (0\ 5\ 4\ 3\ 2\ 1).
\end{aligned}$$

Let us denote the set $\{p_0, p_1, p_2, p_3, p_4, p_5\}$ by P. Then P is a subset of the group of all permutations of the set of symbols $\{0, 1, 2, 3, 4, 5\}$.

We can construct a Cayley table for P by working out all the possible composites of two elements of P. For example,

$$p_1 \circ p_2 = (0\ 1\ 2\ 3\ 4\ 5) \circ (0\ 2\ 4)(1\ 3\ 5) = (0\ 3)(1\ 4)(2\ 5) = p_3.$$

If we do this, then we obtain the following Cayley table for $(P, \circ)$.

$\circ$	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_3	p_4	p_5	p_0
p_2	p_2	p_3	p_4	p_5	p_0	p_1
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_0	p_1	p_2	p_3
p_5	p_5	p_0	p_1	p_2	p_3	p_4

Notice that this Cayley table is exactly the same as the Cayley table for $(\mathbb{Z}_6, +_6)$, except that 0 has been replaced by p_0, and 1 has been replaced by p_1, and so on. In general, each element x of $\mathbb{Z}_6$ has been replaced by p_x. We know that the Cayley table for $(\mathbb{Z}_6, +_6)$ is a group table, so it follows that the Cayley table for $(P, \circ)$ is also a group table (the two tables have exactly the same pattern: it is just that the symbols have different names). It also follows that the following mapping is an isomorphism:

$$\begin{aligned}
\phi : \mathbb{Z}_6 &\longrightarrow P\\
x &\longmapsto p_x.
\end{aligned}$$

So the group $(P, \circ)$ is a representation of the group $(\mathbb{Z}_6, +_6)$ as a permutation group.

Representing any finite group as a permutation group

It turns out that we can use a method similar to that used above for $(\mathbb{Z}_6, +_6)$ to represent *any* finite group as a permutation group. That is, the theorem below holds. Here the symbol $*$ is used instead of our usual symbol $\circ$ to denote the binary operation of a general group G, because the symbol $\circ$ is needed to represent function composition, the binary operation of every permutation group.

Theorem B66

Let $(G, *)$ be a finite group. For each element x of G, let p_x be the permutation whose two-line form has as its first line the column headings of the group table of $(G, *)$ and as its second line the row labelled x in the group table. Let

$$P = \{p_x : x \in G\}.$$

Then $(P, \circ)$ is a permutation group isomorphic to $(G, *)$.

Note that the two-line form for p_x described in Theorem B66 is definitely the two-line form of a *permutation*, as claimed in the statement of the theorem, because each element of G occurs exactly once in the column headings of the group table and, by Proposition B18 in Unit B1, each element of G also occurs exactly once in the row labelled x.

Notice also that the set of symbols being permuted by the permutations specified in Theorem B66 is the set G. So the symbols being permuted may not be numbers.

The following theorem follows immediately from Theorem B66: it is Theorem B66 without the details.

Theorem B67 Cayley's Theorem

Every finite group is isomorphic to a permutation group.

A proof of Theorem B66 (that is, essentially a proof of Cayley's Theorem) is provided at the end of this section for those who are interested.

Theorem B66 is illustrated in the next worked exercise and in the two exercises that follow it.

Worked Exercise B47

Construct a permutation group that is isomorphic to the group $(G, *)$ that has the following group table. Give the permutations in cycle form.

$*$	e	u	v	w	x	z
e	e	u	v	w	x	z
u	u	v	e	z	w	x
v	v	e	u	x	z	w
w	w	x	z	e	u	v
x	x	z	w	v	e	u
z	z	w	x	u	v	e

Solution

For each element of $(G, *)$, we find, in cycle form, the permutation whose two-line form has as its first line the column headings of the group table and as its second line the row of the group table labelled with that element.

$*$	e	u	v	w	x	z		
e	e	u	v	w	x	z	$\longrightarrow$	i (identity)
u	u	v	e	z	w	x	$\longrightarrow$	$(e\ u\ v)(w\ z\ x)$
v	v	e	u	x	z	w	$\longrightarrow$	$(e\ v\ u)(w\ x\ z)$
w	w	x	z	e	u	v	$\longrightarrow$	$(e\ w)(u\ x)(v\ z)$
x	x	z	w	v	e	u	$\longrightarrow$	$(e\ x)(u\ z)(v\ w)$
z	z	w	x	u	v	e	$\longrightarrow$	$(e\ z)(u\ w)(v\ x)$

We do not use e to denote the identity permutation here, as e is already an element of the given group.

A permutation group that is isomorphic to the given group is

$$\{i,\ (e\ u\ v)(w\ z\ x),\ (e\ v\ u)(w\ x\ z),$$
$$(e\ w)(u\ x)(v\ z),\ (e\ x)(u\ z)(v\ w),\ (e\ z)(u\ w)(v\ x)\},$$

where i is the identity permutation.

Exercise B129

Construct a permutation group that is isomorphic to the group that has the following group table. Give the permutations in cycle form.

$\circ$	e	a	b	c	p	q	r	s
e	e	a	b	c	p	q	r	s
a	a	e	c	b	q	p	s	r
b	b	c	a	e	r	s	q	p
c	c	b	e	a	s	r	p	q
p	p	q	s	r	a	e	b	c
q	q	p	r	s	e	a	c	b
r	r	s	p	q	c	b	a	e
s	s	r	q	p	b	c	e	a

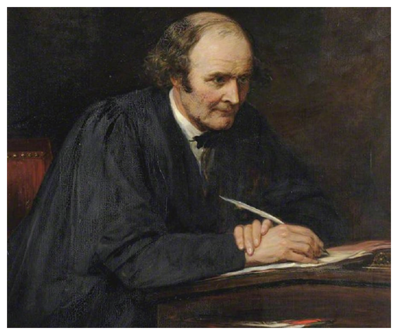
Exercise B130

Construct a permutation group that is isomorphic to the group $(U_8, \times_8)$, that is, $(\{1, 3, 5, 7\}, \times_8)$. Give the permutations in cycle form.

Cayley's Theorem (in its detailed form in Theorem B66), tells us that every finite group of order n is isomorphic to a subgroup of the symmetric group S_n. This is interesting because it suggests that to study finite groups it is sufficient to study only the symmetric groups and their subgroups. However, Cayley's Theorem is not very useful in practice; for example, to study groups of order 8 we would need to consider the subgroups of the symmetric group S_8, which has order $8! = 40\,320$.

Cayley's Theorem can be generalised to infinite groups, but this is beyond the scope of this module.

Cayley's Theorem is named for the British mathematician Arthur Cayley (1821–1895) who in 1854 made the first advance towards the abstract notion of a finite group. Although he implicitly made the connection between group elements and permutations, he did not explicitly prove the theorem, which led to it later being ascribed to Jordan (who proved it in 1870). However, since Cayley communicated the result to the mathematical community at the time, credit for the theorem was soon restored to him.



Arthur Cayley

Proof of Cayley's Theorem (optional)

Here is a proof of Cayley's Theorem. It will not be assessed: read it if you are interested, and skip it if you are not.

To prove Cayley's Theorem we prove Theorem B66, which is as follows.

Theorem B66

Let $(G, *)$ be a finite group. For each element x of G, let p_x be the permutation whose two-line form has as its first line the column headings of the group table of $(G, *)$ and as its second line the row labelled x in the group table. Let

$$P = \{p_x : x \in G\}.$$

Then $(P, \circ)$ is a permutation group isomorphic to $(G, *)$.

Proof Let $G = \{g_1, g_2, g_3, \ldots, g_n\}$. For each element x of G, the row labelled x in the group table of G is as shown below.

$$\begin{array}{c|ccccc}
* & g_1 & g_2 & g_3 & \cdots & g_n \\
\hline
g_1 & & & & & \\
\vdots & & & & & \\
x & x * g_1 & x * g_2 & x * g_3 & \ldots & x * g_n \\
\vdots & & & & & \\
g_n & & & & &
\end{array}$$

Thus, for each element x of G, we have

$$p_x = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ x * g_1 & x * g_2 & \ldots & x * g_n \end{pmatrix}.$$

(As mentioned earlier, the two-line form here is definitely a *permutation*, because each element of G occurs exactly once in the column headings of the group table and exactly once in the row labelled x, by Proposition B18 in Unit B1.)

If x and y are different elements of G, then p_x and p_y are different permutations, since, for example, p_x maps the identity element of G to x whereas p_y maps it to y. Thus the set $P = \{p_x : x \in G\}$ contains the same number of elements as the original group G.

Now let p_x and p_y be any elements of P (not necessarily distinct). We will find a formula for their composite $p_x \circ p_y$ (that is, p_y followed by p_x). We have

$$p_x \circ p_y = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ x * g_1 & x * g_2 & \ldots & x * g_n \end{pmatrix} \circ \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ y * g_1 & y * g_2 & \ldots & y * g_n \end{pmatrix}.$$

To compose the two two-line forms here, we start by finding the image of the symbol g_1 under $p_x \circ p_y$. First, p_y maps g_1 to $y * g_1$. The element $y * g_1$ of G appears somewhere in the top line of the two-line form of p_x and is mapped by p_x to $x * y * g_1$. So $p_x \circ p_y$ maps g_1 to $x * y * g_1$. Similarly, $p_x \circ p_y$ maps g_2 to $x * y * g_2$, and it maps g_3 to $x * y * g_3$, and so on. That is,

$$p_x \circ p_y = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ x * y * g_1 & x * y * g_2 & \cdots & x * y * g_n \end{pmatrix}.$$

But this is the two-line form of the permutation p_{x*y} associated with the element $x * y$ of G. Thus we have the formula

$$p_x \circ p_y = p_{x*y}.$$

We can use this formula to construct a Cayley table for the set P under function composition. It tells us that for each pair of permutations p_x and p_y in P, the entry in the row labelled p_x and column labelled p_y is p_{x*y}, as shown on the right below. We also know that in the Cayley table for the group $(G, *)$, the entry in the row labelled x and column labelled y is $x * y$, as shown on the left below.

$$\begin{array}{c|ccc} * & \cdots & y & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & x*y & \cdots \\ \vdots & & \vdots & \end{array} \qquad\qquad \begin{array}{c|ccc} \circ & \cdots & p_y & \cdots \\ \hline \vdots & & \vdots & \\ p_x & \cdots & p_{x*y} & \cdots \\ \vdots & & \vdots & \end{array}$$

$(G, *)$ $\qquad$ $(P, \circ)$

So the Cayley table for the set P under function composition is exactly the same as the Cayley table of $(G, *)$, except that each element x of G has been replaced by the permutation p_x. We know that the Cayley table for $(G, *)$ is a group table, so it follows that the Cayley table for $(P, \circ)$ is also a group table (the two tables have exactly the same pattern; it is just that the symbols have different names). It also follows that the two groups $(G, *)$ and $(P, \circ)$ are isomorphic, and that the following mapping is an isomorphism:

$$\begin{aligned} \phi : G &\longrightarrow P \\ x &\longmapsto p_x. \end{aligned}$$

This completes the proof. ■

Summary

In this unit you have met the *symmetric groups*, each of which is a group whose elements are all the permutations of a set of symbols $\{1, 2, \ldots, n\}$. The importance of these groups is highlighted by Cayley's Theorem, which states that every group is isomorphic to a subgroup of a symmetric group. You saw that we have been representing the symmetry groups of figures as subgroups of symmetric groups since early in Book B, even though we did not use the terms 'permutation' and 'symmetric group' until this unit. In this unit you have also met the idea of *conjugacy*. Symmetric groups provide a good illustration of this idea, and conjugacy in symmetric groups is important in its own right, but conjugacy is a powerful concept that can usefully be extended to all groups, as you will see in Book E.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *permutation*
- convert a permutation from *two-line form* to *cycle form*
- find a *composite* of two or more permutations and the *inverse* of a permutation
- find the *order* of a permutation
- define the *symmetric group* S_n, and write down the elements of S_3 and S_4
- distinguish between *even* and *odd* permutations
- express a permutation as a composite of transpositions and understand the Parity Theorem
- define the *alternating group* A_n, and write down the elements of A_3 and A_4
- explain the meanings of the terms *conjugate elements* and *conjugate subgroups* in the context of the group S_n
- given any two permutations x and y in S_n with the same cycle structure, find all permutations in S_n that conjugate x to y
- determine subgroups of S_n that are conjugate to a given subgroup
- find all the cyclic subgroups of a particular order in a small symmetric group S_n, given all the elements of that order
- find some non-cyclic subgroups of a symmetric group S_n by finding symmetry groups whose elements can be represented by permutations in S_n
- know Cayley's Theorem
- represent a small finite group as a permutation group by using its group table.

Solutions to exercises

Solution to Exercise B81

(a) We trace the images of the symbols in the order in which they are encountered, starting at the symbol 1.

(i) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

we get

$$1 \longrightarrow 3 \longrightarrow 4 \longrightarrow 2 \longrightarrow 1,$$

so the cycle form is

$$(1\ 3\ 4\ 2).$$

(ii) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 6 & 2 & 1 & 4 \end{pmatrix}$$

we get

$$1 \longrightarrow 5 \longrightarrow 2 \longrightarrow 3 \longrightarrow 7 \longrightarrow 4 \longrightarrow 6 \longrightarrow 1,$$

so the cycle form is

$$(1\ 5\ 2\ 3\ 7\ 4\ 6).$$

(b) Here we carry out the process in part (a) in reverse.

(i) For the cycle $(1\ 3\ 2)$, we get

$$1 \longmapsto 3, \quad 3 \longmapsto 2, \quad 2 \longmapsto 1,$$

so the two-line form is

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

(ii) For the cycle $(1\ 6\ 2\ 4\ 3\ 5)$ we get

$$1 \longmapsto 6, \quad 6 \longmapsto 2, \quad 2 \longmapsto 4, \quad 4 \longmapsto 3,$$
$$3 \longmapsto 5, \quad 5 \longmapsto 1,$$

so the two-line form is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

(c) Starting at the symbol 1 (or 4, 3, 8 or 5) and following the same procedure as in part (a) we get the cycle $(1\ 4\ 3\ 8\ 5)$, which completes after only five symbols. Had we started at the symbol 2, 6 or 7, we would have obtained the cycle $(2\ 6)$ or (7).

So, no matter which symbol we start at, we cannot find a single cycle that contains all eight symbols.

Solution to Exercise B82

(a) Starting the cycle $(1\ 4\ 3\ 8\ 5)$ at 8 we get $(8\ 5\ 1\ 4\ 3)$, and $(2\ 6)$ is the same as $(6\ 2)$, so the cycle form of g may be written as

$$(7)(8\ 5\ 1\ 4\ 3)(6\ 2).$$

(b) Similarly, starting the cycle $(1\ 4\ 3\ 8\ 5)$ at 5 we get $(5\ 1\ 4\ 3\ 8)$, so the cycle form of g may be written as

$$(5\ 1\ 4\ 3\ 8)(2\ 6)(7).$$

Solution to Exercise B83

(*The solution to this exercise contains the details of the process of obtaining the answers, but you need only give the final answers.*)

(a) We trace the images of the symbols in the order in which they are encountered, starting at the symbol 1.

(i) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 1 & 5 & 3 \end{pmatrix},$$

we get

$$1 \longrightarrow 2 \longrightarrow 6 \longrightarrow 3 \longrightarrow 4 \longrightarrow 1;$$

that is, the cycle $(1\ 2\ 6\ 3\ 4)$.

The remaining symbol 5 is mapped to itself. So the cycle form of this permutation is

$$(1\ 2\ 6\ 3\ 4)(5).$$

(ii) For the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 9 & 1 & 3 & 8 & 2 & 6 & 4 \end{pmatrix},$$

we get

$$1 \longrightarrow 5 \longrightarrow 3 \longrightarrow 9 \longrightarrow 4 \longrightarrow 1;$$

that is, the cycle $(1\ 5\ 3\ 9\ 4)$.

The symbol 2 has not yet been placed in a cycle. Starting at 2 we get

$$2 \longrightarrow 7 \longrightarrow 2;$$

that is, the cycle $(2\ 7)$.

The symbol 6 has not yet been placed in a cycle. Starting at 6 we get

$$6 \longrightarrow 8 \longrightarrow 6;$$

that is, the cycle $(6\ 8)$.

All the symbols have now been placed in cycles, so the cycle form of this permutation is

$$(1\ 5\ 3\ 9\ 4)(2\ 7)(6\ 8).$$

(b) **(i)** For the permutation $(1\ 6)(2\ 3\ 7\ 5)(4)$, the cycle form tells us that

$$1 \longmapsto 6, \quad 6 \longmapsto 1;$$
$$2 \longmapsto 3, \quad 3 \longmapsto 7, \quad 7 \longmapsto 5, \quad 5 \longmapsto 2;$$
$$4 \longmapsto 4.$$

We have now found the image of each symbol, so the two-line form for this permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 7 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

(ii) For the permutation $(1\ 6\ 4\ 2)(3\ 5\ 8)(7)$, the cycle form tells us that

$$1 \longmapsto 6, \quad 6 \longmapsto 4, \quad 4 \longmapsto 2, \quad 2 \longmapsto 1;$$
$$3 \longmapsto 5, \quad 5 \longmapsto 8, \quad 8 \longmapsto 3;$$
$$7 \longmapsto 7.$$

We have now found the image of each symbol, so the two-line form for this permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 5 & 2 & 8 & 4 & 7 & 3 \end{pmatrix}.$$

Solution to Exercise B84

The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 4 & 8 & 3 & 6 & 1 & 5 \end{pmatrix}$$

has cycle form

$$(1\ 7)(2)(3\ 4\ 8\ 5)(6),$$

that is,

$$(1\ 7)(3\ 4\ 8\ 5).$$

Solution to Exercise B85

We follow the convention of assuming that symbols in the set $\{1, 2, 3, 4, 5\}$ that are omitted from a cycle form are fixed by the permutation.

(a) The two-line form of the permutation $(1\ 4)(2\ 5)$ is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

(b) The two-line form of the permutation $(1\ 2)$ is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

(c) The two-line form of the permutation $(1\ 5\ 4)$ is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

(d) The two-line form of the permutation e is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Solution to Exercise B86

(*The solution to this exercise contains the details of the process of obtaining the answers, but you need only give the final answers.*)

We use Strategy B8. In each case we start with the symbol 1 and find the cycle containing 1.

As in Worked Exercise B33, the set of symbols is $\{1, 2, 3, 4, 5, 6\}$, and

$$f = (1\ 4\ 3)(2\ 6), \text{ so } f \text{ fixes } 5,$$
$$g = (1\ 4\ 6\ 2\ 5), \text{ so } g \text{ fixes } 3.$$

(a) Remember that $f \circ g$ means 'g first, then f', so

$$(f \circ g)(x) = f(g(x)).$$

For the composite $f \circ g$ we have

$$1 \xrightarrow{g} 4 \text{ and } 4 \xrightarrow{f} 3, \text{ so } 1 \xrightarrow{f \circ g} 3,$$
$$3 \xrightarrow{g} 3 \text{ and } 3 \xrightarrow{f} 1, \text{ so } 3 \xrightarrow{f \circ g} 1.$$

So the composite contains the cycle $(1\ 3)$.

Next we consider the symbol 2:

$$2 \xrightarrow{g} 5 \text{ and } 5 \xrightarrow{f} 5, \text{ so } 2 \xrightarrow{f \circ g} 5,$$
$$5 \xrightarrow{g} 1 \text{ and } 1 \xrightarrow{f} 4, \text{ so } 5 \xrightarrow{f \circ g} 4,$$
$$4 \xrightarrow{g} 6 \text{ and } 6 \xrightarrow{f} 2, \text{ so } 4 \xrightarrow{f \circ g} 2.$$

So the composite contains the cycle $(2\ 5\ 4)$.

Finally,

$$6 \xrightarrow{g} 2 \text{ and } 2 \xrightarrow{f} 6, \text{ so } 6 \xrightarrow{f \circ g} 6.$$

Thus, omitting the 1-cycle (6), we have

$$f \circ g = (1\ 3)(2\ 5\ 4).$$

(b) For the composite $f \circ f$ we have

$$1 \xrightarrow{f} 4 \text{ and } 4 \xrightarrow{f} 3, \text{ so } 1 \xrightarrow{f\circ f} 3,$$
$$3 \xrightarrow{f} 1 \text{ and } 1 \xrightarrow{f} 4, \text{ so } 3 \xrightarrow{f\circ f} 4,$$
$$4 \xrightarrow{f} 3 \text{ and } 3 \xrightarrow{f} 1, \text{ so } 4 \xrightarrow{f\circ f} 1.$$

So the composite contains the cycle (1 3 4).

The permutation f contains the cycle (2 6), so $f \circ f$ fixes both 2 and 6 (since it interchanges them twice).

Finally, f fixes 5, so $f \circ f$ also fixes 5.

Thus

$$f \circ f = (1\ 3\ 4).$$

(c) For the composite $g \circ g$ we have

$$1 \xrightarrow{g} 4 \text{ and } 4 \xrightarrow{g} 6, \text{ so } 1 \xrightarrow{g\circ g} 6,$$
$$6 \xrightarrow{g} 2 \text{ and } 2 \xrightarrow{g} 5, \text{ so } 6 \xrightarrow{g\circ g} 5,$$
$$5 \xrightarrow{g} 1 \text{ and } 1 \xrightarrow{g} 4, \text{ so } 5 \xrightarrow{g\circ g} 4,$$
$$4 \xrightarrow{g} 6 \text{ and } 6 \xrightarrow{g} 2, \text{ so } 4 \xrightarrow{g\circ g} 2,$$
$$2 \xrightarrow{g} 5 \text{ and } 5 \xrightarrow{g} 1, \text{ so } 2 \xrightarrow{g\circ g} 1.$$

So the composite contains the cycle (1 6 5 4 2).

Finally, g fixes 3, so $g \circ g$ also fixes 3.

Thus

$$g \circ g = (1\ 6\ 5\ 4\ 2).$$

Solution to Exercise B87

We use Strategy B8. Notice that the set is $\{1, 2, 3, 4, 5, 6\}$, and

$$f = (1\ 3\ 2\ 4\ 6), \text{ so } f \text{ fixes } 5,$$
$$g = (1\ 4)(3\ 5), \text{ so } g \text{ fixes 2 and 6}.$$

(a) $g \circ f = (1\ 4)(3\ 5) \circ (1\ 3\ 2\ 4\ 6)$
$= (1\ 5\ 3\ 2)(4\ 6).$

(b) $f \circ g = (1\ 3\ 2\ 4\ 6) \circ (1\ 4)(3\ 5)$
$= (1\ 6)(2\ 4\ 3\ 5).$

(c) $f \circ f = (1\ 3\ 2\ 4\ 6) \circ (1\ 3\ 2\ 4\ 6)$
$= (1\ 2\ 6\ 3\ 4).$

(d) The permutation g consists of cycles each of which interchanges two symbols. Performing such a cycle twice interchanges the two symbols twice, so $g \circ g = e$.

Solution to Exercise B88

We use Strategy B8, adapted to apply to three or more permutations.

(a) We have

$$(1\ 3)(2\ 4)(5\ 7\ 6) \circ (1\ 7\ 6)(2\ 3) \circ (1\ 7\ 4\ 6)$$
$$= (1\ 5\ 7\ 2)(3\ 4)(6) = (1\ 5\ 7\ 2)(3\ 4).$$

(b) Here

$$(1\ 7\ 3\ 4\ 6) \circ (1\ 2) \circ (3\ 7) \circ (5\ 3)$$
$$= (1\ 2\ 7\ 4\ 6)(3\ 5).$$

Solution to Exercise B89

Following Strategy B9 we obtain the inverse by writing each cycle in reverse order.

(a) $(1\ 6\ 4\ 2\ 5\ 8\ 3\ 7)^{-1} = (7\ 3\ 8\ 5\ 2\ 4\ 6\ 1)$
$= (1\ 7\ 3\ 8\ 5\ 2\ 4\ 6)$

(b) $((1\ 5\ 4\ 7)(2\ 6\ 8))^{-1} = (7\ 4\ 5\ 1)(8\ 6\ 2)$
$= (1\ 7\ 4\ 5)(2\ 8\ 6)$

(c) $((1\ 8)(2\ 7)(3\ 5))^{-1} = (8\ 1)(7\ 2)(5\ 3)$
$= (1\ 8)(2\ 7)(3\ 5).$

Notice that the permutation (1 8)(2 7)(3 5) is its own inverse. This is because each of its cycles interchanges two symbols.

Solution to Exercise B90

(a) In part (i) we use Strategy B8 and in parts (ii)–(iv) we use Strategy B9.

(i) $g \circ f = (1\ 5\ 3\ 6\ 2)$

(ii) $f^{-1} = (5\ 4\ 6\ 2\ 1)$
$= (1\ 5\ 4\ 6\ 2)$

(iii) $g^{-1} = (6\ 3\ 1)(4\ 5\ 2)$
$= (1\ 6\ 3)(2\ 4\ 5)$

(iv) $(g \circ f)^{-1} = (1\ 5\ 3\ 6\ 2)^{-1} = (2\ 6\ 3\ 5\ 1)$
$= (1\ 2\ 6\ 3\ 5)$

(b) Strategy B8 gives

$$\begin{aligned} f^{-1} \circ g^{-1} &= (1\ 5\ 4\ 6\ 2) \circ (1\ 6\ 3)(2\ 4\ 5) \\ &= (1\ 2\ 6\ 3\ 5), \end{aligned}$$

which is the expression for $(g \circ f)^{-1}$ that was found in part (a)(iv).

(Remember that the equation

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

holds for any two one-to-one functions f and g, as mentioned immediately after the proof of Proposition B14 in Unit B1.)

Solution to Exercise B91

(a) In two-line form, the elements of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

In cycle form, they are

$$e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2).$$

Thus S_3 has order 6.

(b) We count how many different ways there are to complete the bottom row of the two-line form of a permutation of the set $\{1, 2, 3, 4\}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}.$$

There are 4 choices for the symbol to be placed in the first position in the bottom row.

Once we have chosen this symbol, there are only 3 symbols still to be placed, so there are 3 choices for the symbol to be placed in the second position.

Once we have chosen the first two symbols, there are only 2 symbols still to be placed, so there are 2 choices for the symbol to be placed in the third position.

Finally, there is just 1 choice left for the symbol to be placed in the fourth position.

The total number of ways to complete the bottom row is therefore

$$4 \times 3 \times 2 \times 1 = 4! = 24.$$

That is, the group S_4 has order 24.

(The number of ways to fill in the bottom row is the number of permutations of 4 symbols from 4, in the sense in which the word 'permutation' is used in combinatorics. You may know that this is written as ${}^4P_4$, and is equal to $4! = 24$.)

Solution to Exercise B92

There are five possible cycle structures in S_4. A representative permutation for each cycle structure is given in the following table.

Cycle structure	Element of S_4	Description
e	e	identity
$(-\ -)$	$(1\ 2)$	transposition
$(-\ -\ -)$	$(1\ 2\ 3)$	3-cycle
$(-\ -\ -\ -)$	$(1\ 2\ 3\ 4)$	4-cycle
$(-\ -)(-\ -)$	$(1\ 2)(3\ 4)$	two 2-cycles

Solution to Exercise B93

There are seven possible cycle structures in S_5. A representative permutation for each cycle structure is given in the following table.

Cycle structure	Element of S_5	Description
e	e	identity
$(-\ -)$	$(1\ 2)$	transposition
$(-\ -\ -)$	$(1\ 2\ 3)$	3-cycle
$(-\ -\ -\ -)$	$(1\ 2\ 3\ 4)$	4-cycle
$(-\ -\ -\ -\ -)$	$(1\ 2\ 3\ 4\ 5)$	5-cycle
$(-\ -)(-\ -)$	$(1\ 2)(3\ 4)$	two 2-cycles
$(-\ -)(-\ -\ -)$	$(1\ 2)(3\ 4\ 5)$	2-cycle and 3-cycle

Solution to Exercise B94

For the permutation $f = (1\ 6\ 3\ 7\ 5\ 2)$,

$$\begin{aligned} f^2 &= (1\ 3\ 5)(2\ 6\ 7), \\ f^3 &= (1\ 7)(2\ 3)(5\ 6), \\ f^4 &= (1\ 5\ 3)(2\ 7\ 6), \\ f^5 &= (1\ 2\ 5\ 7\ 3\ 6), \\ f^6 &= e. \end{aligned}$$

So the 6-cycle f has order 6.

Solution to Exercise B95

By Theorem B55, the order of a permutation is the least common multiple of the lengths of its cycles.

(a) The cycle lengths are 4, 2 and 2, so the order is 4.

(b) The cycle lengths are 3 and 5, so the order is 15.

(c) The cycle lengths are 2, 2, 2 and 3, so the order is 6.

(d) The cycle lengths are 3 and 3, so the order is 3.

Solution to Exercise B96

(a) The permutation $(1\ 5\ 2\ 3)$ has order 4, so

$$\begin{aligned}&\langle(1\ 5\ 2\ 3)\rangle\\ &= \{e, (1\ 5\ 2\ 3), (1\ 5\ 2\ 3)^2, (1\ 5\ 2\ 3)^3\}\\ &= \{e, (1\ 5\ 2\ 3), (1\ 2)(3\ 5), (1\ 3\ 2\ 5)\}.\end{aligned}$$

(b) The permutation $(1\ 4\ 2)(3\ 5)$ has order 6, so

$$\begin{aligned}&\langle(1\ 4\ 2)(3\ 5)\rangle\\ &= \{e, (1\ 4\ 2)(3\ 5), ((1\ 4\ 2)(3\ 5))^2,\\ &\qquad ((1\ 4\ 2)(3\ 5))^3, ((1\ 4\ 2)(3\ 5))^4,\\ &\qquad ((1\ 4\ 2)(3\ 5))^5\}\\ &= \{e, (1\ 4\ 2)(3\ 5), (1\ 2\ 4), (3\ 5), (1\ 4\ 2),\\ &\qquad (1\ 2\ 4)(3\ 5)\}.\end{aligned}$$

Solution to Exercise B97

The set S is a subset of S_6, since its elements permute the symbols 1, 2, 3, 4, 5 and 6 (fixing 2, 3 and 4). Also, the permutation $(1\ 5\ 6)$ has order 3, so

$$\begin{aligned}\langle(1\ 5\ 6)\rangle &= \{e, (1\ 5\ 6), (1\ 5\ 6)^2\}\\ &= \{e, (1\ 5\ 6), (1\ 6\ 5)\}\\ &= S.\end{aligned}$$

Hence S is the cyclic subgroup of S_6 generated by $(1\ 5\ 6)$; in particular, it is a subgroup of S_6.

Solution to Exercise B98

The symmetries in $S(\triangle)$ and their orders are shown below.

	Symmetry	Order
Rotations	e	1
	$a = (1\ 2\ 3)$	3
	$b = (1\ 3\ 2)$	3
Reflections	$r = (2\ 3)$	2
	$s = (1\ 3)$	2
	$t = (1\ 2)$	2

Solution to Exercise B99

The symmetries in $S(\square)$ and their orders are shown below.

	Symmetry	Order
Rotations	e	1
	$a = (1\ 3)(2\ 4)$	2
Reflections	$r = (1\ 4)(2\ 3)$	2
	$s = (1\ 2)(3\ 4)$	2

Solution to Exercise B100

The symmetries of the hexagon and their orders are shown below.

	Symmetry	Order
Rotations	e	1
	$(1\ 2\ 3\ 4\ 5\ 6)$	6
	$(1\ 3\ 5)(2\ 4\ 6)$	3
	$(1\ 4)(2\ 5)(3\ 6)$	2
	$(1\ 5\ 3)(2\ 6\ 4)$	3
	$(1\ 6\ 5\ 4\ 3\ 2)$	6
Reflections	$(1\ 6)(2\ 5)(3\ 4)$	2
	$(1\ 2)(3\ 6)(4\ 5)$	2
	$(1\ 4)(2\ 3)(5\ 6)$	2
	$(2\ 6)(3\ 5)$	2
	$(1\ 3)(4\ 6)$	2
	$(1\ 5)(2\ 4)$	2

Solution to Exercise B101

The symmetries of the figure are represented by the following permutations in S_3:

$$e,\ (1\ 2\ 3),\ (1\ 3\ 2).$$

(Since the symmetries form a group, these three symmetries form a subgroup of S_3.)

Solution to Exercise B102

A subgroup of S_5 is

$$\{e,\ (1\ 4)(2\ 5),\ (1\ 5)(2\ 4),\ (1\ 2)(4\ 5)\}.$$

Solution to Exercise B103

The identity symmetry e fixes all four edges.

The rotation through a half turn transposes opposite pairs of edges, namely 1, 2 and 3, 4, so

$$a = (1\ 2)(3\ 4).$$

Reflection in the vertical axis of symmetry maps the edges 1 and 2 to themselves and transposes the edges 3 and 4, so

$$r = (3\ 4).$$

Reflection in the horizontal axis of symmetry maps the edges 3 and 4 to themselves and transposes the edges 1 and 2, so

$$s = (1\ 2).$$

So, with this labelling of the rectangle, the symmetry group is

$$\{e,\ (1\ 2)(3\ 4),\ (3\ 4),\ (1\ 2)\}.$$

Solution to Exercise B104

The symmetries of the double tetrahedron are represented by the following permutations in S_6.

e	$(1\ 4)(2\ 5)(3\ 6)$
$(1\ 2\ 3)(4\ 5\ 6)$	$(1\ 5\ 3\ 4\ 2\ 6)$
$(1\ 3\ 2)(4\ 6\ 5)$	$(1\ 6\ 2\ 4\ 3\ 5)$
$(1\ 2)(4\ 5)$	$(1\ 5)(2\ 4)(3\ 6)$
$(1\ 3)(4\ 6)$	$(1\ 6)(2\ 5)(3\ 4)$
$(2\ 3)(5\ 6)$	$(1\ 4)(2\ 6)(3\ 5)$

(The permutations in the first column are the symmetries obtained from the symmetries of the equilateral triangle in the middle of the double tetrahedron. The first symmetry in the second column is the reflection in the horizontal plane through the middle of the double tetrahedron. The remaining symmetries in the second column are obtained by composing each of the permutations in the first column with the first permutation in the second column, in that order.)

Solution to Exercise B105

(a) (*The solution to this exercise contains the details of the process of obtaining the answers, but you need only give the final answers.*)

In each case we find the image of each symbol in turn, starting with the symbol 1.

(i) For the composite $(1\ 4) \circ (1\ 2)$ we have

$$1 \longmapsto 2,\ \text{then}\ 2 \longmapsto 2,\ \text{so}\ 1 \longmapsto 2;$$
$$2 \longmapsto 1,\ \text{then}\ 1 \longmapsto 4,\ \text{so}\ 2 \longmapsto 4;$$
$$4 \longmapsto 4,\ \text{then}\ 4 \longmapsto 1,\ \text{so}\ 4 \longmapsto 1.$$

Thus

$$(1\ 4) \circ (1\ 2) = (1\ 2\ 4).$$

(ii) For the composite $(1\ 3) \circ (1\ 2) \circ (1\ 4)$ we have

$$1 \longmapsto 4,\ \text{then}\ 4 \longmapsto 4,\ \text{then}\ 4 \longmapsto 4,\ \text{so}\ 1 \longmapsto 4;$$
$$4 \longmapsto 1,\ \text{then}\ 1 \longmapsto 2,\ \text{then}\ 2 \longmapsto 2,\ \text{so}\ 4 \longmapsto 2;$$
$$2 \longmapsto 2,\ \text{then}\ 2 \longmapsto 1,\ \text{then}\ 1 \longmapsto 3,\ \text{so}\ 2 \longmapsto 3;$$
$$3 \longmapsto 3,\ \text{then}\ 3 \longmapsto 3,\ \text{then}\ 3 \longmapsto 1,\ \text{so}\ 3 \longmapsto 1.$$

Thus

$$(1\ 3) \circ (1\ 2) \circ (1\ 4) = (1\ 4\ 2\ 3).$$

(iii) For the composite $(3\ 1) \circ (3\ 4) \circ (3\ 2)$ we have

$$1 \longmapsto 1,\ \text{then}\ 1 \longmapsto 1,\ \text{then}\ 1 \longmapsto 3,\ \text{so}\ 1 \longmapsto 3;$$
$$3 \longmapsto 2,\ \text{then}\ 2 \longmapsto 2,\ \text{then}\ 2 \longmapsto 2,\ \text{so}\ 3 \longmapsto 2;$$
$$2 \longmapsto 3,\ \text{then}\ 3 \longmapsto 4,\ \text{then}\ 4 \longmapsto 4,\ \text{so}\ 2 \longmapsto 4;$$
$$4 \longmapsto 4,\ \text{then}\ 4 \longmapsto 3,\ \text{then}\ 3 \longmapsto 1,\ \text{so}\ 4 \longmapsto 1.$$

Thus

$$(3\ 1) \circ (3\ 4) \circ (3\ 2) = (1\ 3\ 2\ 4).$$

(b) In part (a) we found that

$$(1\ 4) \circ (1\ 2) = (1\ 2\ 4),$$
$$(1\ 3) \circ (1\ 2) \circ (1\ 4) = (1\ 4\ 2\ 3),$$
$$(3\ 1) \circ (3\ 4) \circ (3\ 2) = (3\ 2\ 4\ 1).$$

(The last cycle has been reordered to make the pattern obvious.)

In each case the composite is a cycle in which the symbol common to all the transpositions is followed by the other symbols from the transpositions *in their order of appearance from right to left.*

Using this pattern we obtain the following, which can be checked by composing the transpositions:

$$(1\ 4\ 3) = (1\ 3) \circ (1\ 4),$$

$$(1\ 4\ 3\ 2) = (1\ 2) \circ (1\ 3) \circ (1\ 4).$$

Solution to Exercise B106

Following Strategy B10 we obtain the following.

(a) $(1\ 5\ 2\ 7\ 3) = (1\ 3) \circ (1\ 7) \circ (1\ 2) \circ (1\ 5)$

(b) $(2\ 3\ 7\ 5\ 4\ 6) = (2\ 6) \circ (2\ 4) \circ (2\ 5) \circ (2\ 7) \circ (2\ 3)$

(c) $(1\ 2\ 3\ 4\ 5\ 6\ 7)$
$= (1\ 7) \circ (1\ 6) \circ (1\ 5) \circ (1\ 4) \circ (1\ 3) \circ (1\ 2)$

Solution to Exercise B107

(a) A 4-cycle is a composite of three transpositions:

$$(a_1\ a_2\ a_3\ a_4) = (a_1\ a_4) \circ (a_1\ a_3) \circ (a_1\ a_2).$$

(b) A 5-cycle is a composite of four transpositions:

$$\begin{aligned}&(a_1\ a_2\ a_3\ a_4\ a_5)\\&= (a_1\ a_5) \circ (a_1\ a_4) \circ (a_1\ a_3) \circ (a_1\ a_2).\end{aligned}$$

(c) An r-cycle is a composite of $r-1$ transpositions:

$$\begin{aligned}&(a_1\ a_2\ \ldots\ a_{r-1}\ a_r)\\&= (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \cdots \circ (a_1\ a_2).\end{aligned}$$

Solution to Exercise B108

We use the method of Worked Exercise B41.

(a) $$\begin{aligned}&(1\ 8\ 3)(2\ 6\ 5\ 7)\\&= (1\ 8\ 3) \circ (2\ 6\ 5\ 7)\\&= (1\ 3) \circ (1\ 8) \circ (2\ 7) \circ (2\ 5) \circ (2\ 6).\end{aligned}$$

(b) $$\begin{aligned}&(1\ 7)(2\ 6\ 8)(3\ 4\ 5)\\&= (1\ 7) \circ (2\ 6\ 8) \circ (3\ 4\ 5)\\&= (1\ 7) \circ (2\ 8) \circ (2\ 6) \circ (3\ 5) \circ (3\ 4).\end{aligned}$$

Solution to Exercise B109

(a) We apply Theorem B59.

The permutation $(1\ 2\ 5\ 3)$ is a 4-cycle and so is odd.

The permutation $(1\ 6\ 2\ 5\ 4)$ is a 5-cycle and so is even.

(b) The solution to Exercise B108 shows that the permutation $(1\ 8\ 3)(2\ 6\ 5\ 7)$ can be expressed as a composite of five transpositions and so is an odd permutation.

It also shows that the permutation $(1\ 7)(2\ 6\ 8)(3\ 4\ 5)$ can be expressed as a composite of five transpositions and so is an odd permutation.

(c) We use Strategy B10 to express the two cycles as composites of transpositions. This gives

$$\begin{aligned}&(1\ 8\ 2\ 7\ 6)(3\ 5\ 9\ 4)\\&= (1\ 8\ 2\ 7\ 6) \circ (3\ 5\ 9\ 4)\\&= (1\ 6) \circ (1\ 7) \circ (1\ 2) \circ (1\ 8) \circ (3\ 4) \circ (3\ 9) \circ (3\ 5).\end{aligned}$$

So $(1\ 8\ 2\ 7\ 6)(3\ 5\ 9\ 4)$ can be expressed as a composite of seven transpositions and so is an odd permutation.

Solution to Exercise B110

(a) Here

$$(1\ 2\ 4)(3\ 5) \circ (1\ 5\ 2) = (1\ 2\ 4) \circ (3\ 5) \circ (1\ 5\ 2).$$

The cycles of the expression on the right-hand side of this equation are respectively even, odd and even. Combining parities we obtain

$$\text{even} + \text{odd} + \text{even} = \text{odd}.$$

Thus $(1\ 2\ 4)(3\ 5) \circ (1\ 5\ 2)$ is an odd permutation.

(b) Here

$$\begin{aligned}&(1\ 2\ 4) \circ (1\ 3)(2\ 5\ 4) \circ (1\ 2\ 3\ 4)\\&= (1\ 2\ 4) \circ (1\ 3) \circ (2\ 5\ 4) \circ (1\ 2\ 3\ 4).\end{aligned}$$

The cycles of the expression on the right-hand side of this equation are respectively even, odd, even and odd, so we obtain

$$\text{even} + \text{odd} + \text{even} + \text{odd} = \text{even}.$$

Thus $(1\ 2\ 4) \circ (1\ 3)(2\ 5\ 4) \circ (1\ 2\ 3\ 4)$ is an even permutation.

Solution to Exercise B111

$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.

(The other three elements of S_3 are the transpositions, which are odd permutations.)

Thus A_3 has order 3.

Solution to Exercise B112

(a) The cycle number of f is 1.

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 4\ 5\ 2\ 3\ 6\ 7) \\ &= (1\ 4\ 5)(2\ 3\ 6\ 7) \end{aligned}$$

So the cycle number of $t \circ f$ is 2.

(b) The cycle number of f is 2.

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 4\ 3)(2\ 6\ 5\ 7) \\ &= (1\ 4\ 3\ 2\ 6\ 5\ 7) \end{aligned}$$

So the cycle number of $t \circ f$ is 1.

(c) The cycle number of f is 3. (Since f is $(1\ 2\ 7\ 3)(4\ 6)(5)$ with 1-cycles included.)

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 2\ 7\ 3)(4\ 6) \\ &= (1)(2\ 7\ 3)(4\ 6) \\ &= (2\ 7\ 3)(4\ 6) \end{aligned}$$

So the cycle number of $t \circ f$ is 4. (It has a 3-cycle, a 2-cycle and two 1-cycles.)

(d) The cycle number of f is 3.

$$\begin{aligned} t \circ f &= (1\ 2) \circ (1\ 5\ 3)(2\ 4)(6\ 7) \\ &= (1\ 5\ 3\ 2\ 4)(6\ 7) \end{aligned}$$

So the cycle number of $t \circ f$ is 2.

Solution to Exercise B113

The original permutations are as follows.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 2\ 3\ 4)$	$(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$
$(1\ 4\ 3\ 2)$	$(1\ 3)$

(a) The permutations obtained by relabelling the vertex locations using the transposition $(3\ 4)$, that is, by interchanging 3 and 4, are as follows.

Rotations	Reflections
e	$(1\ 3)(2\ 4)$
$(1\ 2\ 4\ 3)$	$(2\ 3)$
$(1\ 4)(2\ 3)$	$(1\ 2)(4\ 3)$
$(1\ 3\ 4\ 2)$	$(1\ 4)$

(b) The permutations obtained by relabelling the vertex locations using the permutation $(2\ 3\ 4)$, that is, by keeping 1 fixed and replacing 2 by 3, 3 by 4 and 4 by 2, are as follows.

Rotations	Reflections
e	$(1\ 2)(3\ 4)$
$(1\ 3\ 4\ 2)$	$(3\ 2)$
$(1\ 4)(3\ 2)$	$(1\ 3)(4\ 2)$
$(1\ 2\ 4\ 3)$	$(1\ 4)$

Here one of the reflections, $(3\ 2)$, is not written in the usual way. If we write it in the usual way, then we obtain the following list of permutations.

Rotations	Reflections
e	$(1\ 2)(3\ 4)$
$(1\ 3\ 4\ 2)$	$(2\ 3)$
$(1\ 4)(3\ 2)$	$(1\ 3)(4\ 2)$
$(1\ 2\ 4\ 3)$	$(1\ 4)$

(Notice that the list of permutations found in part (b) is in fact exactly the same as the list found in part (a).)

Solution to Exercise B114

(a) Here $g = (1\ 4)(2\ 5\ 3)$, so $g^{-1} = (4\ 1)(3\ 5\ 2)$ which, when rewritten in the usual way, is $(1\ 4)(2\ 3\ 5)$. Thus

$$\begin{aligned} &g \circ x \circ g^{-1} \\ &= (1\ 4)(2\ 5\ 3) \circ (1\ 2\ 3\ 5) \circ (1\ 4)(2\ 3\ 5) \\ &= (1)(2\ 3\ 4\ 5) \\ &= (2\ 3\ 4\ 5). \end{aligned}$$

Using $g = (1\ 4)(2\ 5\ 3)$ to rename $x = (1\ 2\ 3\ 5)$, we obtain $(4\ 5\ 2\ 3)$, which is the same 4-cycle as above.

(b) Here $g = (1\ 3\ 4\ 2\ 5)$, so $g^{-1} = (5\ 2\ 4\ 3\ 1)$ which, when rewritten in the usual way, is $(1\ 5\ 2\ 4\ 3)$. Thus

$$\begin{aligned} &g \circ x \circ g^{-1} \\ &= (1\ 3\ 4\ 2\ 5) \circ (1\ 2\ 3\ 5) \circ (1\ 5\ 2\ 4\ 3) \\ &= (1\ 3\ 5\ 4)(2) \\ &= (1\ 3\ 5\ 4). \end{aligned}$$

Using $g = (1\ 3\ 4\ 2\ 5)$ to rename $x = (1\ 2\ 3\ 5)$, we obtain $(3\ 5\ 4\ 1)$, which is the same 4-cycle as above.

Solution to Exercise B115

We obtain three more answers by writing y in the following three ways:

$$(2\ 5\ 3)(4\ 1), \quad (3\ 2\ 5)(4\ 1), \quad (5\ 3\ 2)(1\ 4).$$

With the first way above we obtain

$$\begin{array}{rl} x = & (1\ 2\ 4)(3\ 5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ y = & (2\ 5\ 3)(4\ 1) \end{array},$$

which gives $g = (1\ 2\ 5)(3\ 4)$.

With the second way we obtain

$$\begin{array}{rl} x = & (1\ 2\ 4)(3\ 5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ y = & (3\ 2\ 5)(4\ 1) \end{array},$$

which gives $g = (1\ 3\ 4\ 5)$.

Finally, with the third way we obtain

$$\begin{array}{rl} x = & (1\ 2\ 4)(3\ 5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ y = & (5\ 3\ 2)(1\ 4) \end{array},$$

which gives $g = (1\ 5\ 4\ 2\ 3)$.

Solution to Exercise B116

(a) Here $x = (1\ 2\ 3\ 4)(5)$ and $y = (1\ 5\ 2\ 3)(4)$. We can write the cycle in $(1\ 5\ 2\ 3)$ in y in four ways:

$$(1\ 5\ 2\ 3),\ (5\ 2\ 3\ 1),\ (2\ 3\ 1\ 5),\ (3\ 1\ 5\ 2).$$

Writing y as $(1\ 5\ 2\ 3)(4)$ and matching up the cycles we obtain

$$\begin{array}{rl} x = & (1\ 2\ 3\ 4)(5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \ \downarrow \\ y = & (1\ 5\ 2\ 3)(4) \end{array}, \text{ which gives } g = (2\ 5\ 4\ 3).$$

Similarly, for the other three ways of writing y we obtain

$$\begin{array}{rl} x = & (1\ 2\ 3\ 4)(5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \ \downarrow \\ y = & (5\ 2\ 3\ 1)(4) \end{array}, \text{ which gives } g = (1\ 5\ 4);$$

$$\begin{array}{rl} x = & (1\ 2\ 3\ 4)(5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \ \downarrow \\ y = & (2\ 3\ 1\ 5)(4) \end{array}, \text{ which gives } g = (1\ 2\ 3)(4\ 5);$$

$$\begin{array}{rl} x = & (1\ 2\ 3\ 4)(5) \\ g\downarrow & \ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \ \downarrow \\ y = & (3\ 1\ 5\ 2)(4) \end{array}, \text{ which gives } g = (1\ 3\ 5\ 4\ 2).$$

(b) There are eight different ways of writing the permutation $(1\ 2)(3\ 4)$ underneath itself with the cycles matched up. (There are 2 ways to write each of the two cycles, and 2 ways to order the two cycles, so the number of suitable ways to write the permutation is $2 \times 2 \times 2 = 8$.)

Writing it in these eight possible ways we obtain

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (1\ 2)(3\ 4) \end{array}, \text{ which gives } g = e;$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (2\ 1)(3\ 4) \end{array}, \text{ which gives } g = (1\ 2);$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (1\ 2)(4\ 3) \end{array}, \text{ which gives } g = (3\ 4);$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (2\ 1)(4\ 3) \end{array}, \text{ which gives } g = (1\ 2)(3\ 4);$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (3\ 4)(1\ 2) \end{array}, \text{ which gives } g = (1\ 3)(2\ 4);$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (4\ 3)(1\ 2) \end{array}, \text{ which gives } g = (1\ 4\ 2\ 3);$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (3\ 4)(2\ 1) \end{array}, \text{ which gives } g = (1\ 3\ 2\ 4);$$

$$\begin{array}{rl} & (1\ 2)(3\ 4) \\ g & \ \downarrow\ \downarrow\ \ \downarrow\ \downarrow \\ & (4\ 3)(2\ 1) \end{array}, \text{ which gives } g = (1\ 4)(2\ 3).$$

Solution to Exercise B117

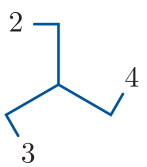
(a) Renaming the symbols in each permutation in H using the permutation $g = (1\ 4)(2\ 5)$ gives

$$\begin{aligned} g \circ H \circ g^{-1} &= \{e, (4\ 3\ 2), (4\ 2\ 3)\} \\ &= \{e, (2\ 4\ 3), (2\ 3\ 4)\}. \end{aligned}$$

(b) The set $g \circ H \circ g^{-1}$ is a subgroup of S_5 because it is the cyclic subgroup of S_5 generated by the 3-cycle $(2\ 4\ 3)$:

$$\begin{aligned} \langle (2\ 4\ 3) \rangle &= \{e, (2\ 4\ 3), (2\ 4\ 3)^2\} \\ &= \{e, (2\ 4\ 3), (2\ 3\ 4)\} \\ &= g \circ H \circ g^{-1}. \end{aligned}$$

(There are other ways to show that $g \circ H \circ g^{-1}$ is a subgroup of S_5. For example, you could construct a Cayley table for this set and use the usual subgroup test (Theorem B24 in Unit B2). Alternatively, you could argue that the elements of the set $g \circ H \circ g^{-1}$ represent the symmetries of the labelled figure below, with the symbols 1 and 5 being fixed.)



Solution to Exercise B118

Here $H = \{e, (1\ 2\ 5\ 3), (1\ 5)(2\ 3), (1\ 3\ 5\ 2)\}$.

(a) To find $(1\ 3) \circ H \circ (1\ 3)^{-1}$ we interchange the symbols 1 and 3 in the elements of H, which gives

$$\begin{aligned} &(1\ 3) \circ H \circ (1\ 3)^{-1} \\ &= \{e, (3\ 2\ 5\ 1), (3\ 5)(2\ 1), (3\ 1\ 5\ 2)\} \\ &= \{e, (1\ 3\ 2\ 5), (1\ 2)(3\ 5), (1\ 5\ 2\ 3)\}. \end{aligned}$$

(b) To find $(1\ 3)(2\ 4) \circ H \circ ((1\ 3)(2\ 4))^{-1}$ we replace 1 by 3, 3 by 1, 2 by 4 and 4 by 2 in the elements of H, which gives

$$\begin{aligned} &(1\ 3)(2\ 4) \circ H \circ ((1\ 3)(2\ 4))^{-1} \\ &= \{e, (3\ 4\ 5\ 1), (3\ 5)(4\ 1), (3\ 1\ 5\ 4)\} \\ &= \{e, (1\ 3\ 4\ 5), (1\ 4)(3\ 5), (1\ 5\ 4\ 3)\}. \end{aligned}$$

Solution to Exercise B119

(a) There are three permutations g that conjugate $(1\ 2\ 3)$ to itself, corresponding to the three ways of writing $(1\ 2\ 3)$, as shown in the following table.

Form of $(1\ 2\ 3)$	Conjugating permutation
$(1\ 2\ 3)$	e
$(2\ 3\ 1)$	$(1\ 2\ 3)$
$(3\ 1\ 2)$	$(1\ 3\ 2)$

These three conjugating permutations are the elements of the subgroup A_3 of S_3.

(An alternative way to show that the three conjugating permutations above form a subgroup of S_3 is to show that they are the elements of the cyclic subgroup of S_3 generated by the permutation $(1\ 2\ 3)$.)

(b) There are four permutations g that conjugate $(1\ 2\ 3\ 4)$ to itself, corresponding to the four ways of writing $(1\ 2\ 3\ 4)$, as shown in the following table.

Form of $(1\ 2\ 3\ 4)$	Conjugating permutation
$(1\ 2\ 3\ 4)$	e
$(2\ 3\ 4\ 1)$	$(1\ 2\ 3\ 4)$
$(3\ 4\ 1\ 2)$	$(1\ 3)(2\ 4)$
$(4\ 1\ 2\ 3)$	$(1\ 4\ 3\ 2)$

Now $(1\ 2\ 3\ 4)$ has order 4 and

$$\begin{aligned} (1\ 2\ 3\ 4)^2 &= (1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4), \\ &= (1\ 3)(2\ 4), \end{aligned}$$

$$\begin{aligned} (1\ 2\ 3\ 4)^3 &= (1\ 2\ 3\ 4) \circ (1\ 2\ 3\ 4)^2 \\ &= (1\ 2\ 3\ 4) \circ (1\ 3)(2\ 4) \\ &= (1\ 4\ 3\ 2). \end{aligned}$$

So the four conjugating permutations form the cyclic subgroup of S_4 generated by $(1\ 2\ 3\ 4)$:

$$\begin{aligned} &\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\} \\ &= \langle (1\ 2\ 3\ 4) \rangle. \end{aligned}$$

Solution to Exercise B120

We show that C satisfies the three subgroup properties SG1, SG2 and SG3.

SG1 Let g_1 and g_2 be any two elements of C; then

$$g_1 \circ f \circ g_1^{-1} = f$$

and

$$g_2 \circ f \circ g_2^{-1} = f.$$

Substituting the second of these equations into the first gives

$$g_1 \circ g_2 \circ f \circ g_2^{-1} \circ g_1^{-1} = f;$$

that is (by Proposition B14 in Unit B1),

$$(g_1 \circ g_2) \circ f \circ (g_1 \circ g_2)^{-1} = f.$$

This shows that $g_1 \circ g_2$ is in C, so C is closed under $\circ$.

SG2 We have $e \circ f \circ e^{-1} = f$, so $e \in C$.

SG3 Let g be any element of C; then

$$g \circ f \circ g^{-1} = f.$$

Composing both sides of this equation on the left by g^{-1} and on the right by g gives

$$g^{-1} \circ g \circ f \circ g^{-1} \circ g = g^{-1} \circ f \circ g.$$

This equation simplifies to give

$$f = g^{-1} \circ f \circ g,$$

which can be written as

$$g^{-1} \circ f \circ (g^{-1})^{-1} = f.$$

This shows that g^{-1} is in C, so C contains the inverse of each of its elements.

Hence C satisfies the three subgroup properties and so is a subgroup of G.

(The condition $g \circ f \circ g^{-1} = f$ is equivalent to the condition $g \circ f = f \circ g$, so C is the set of all elements of G that *commute* with the fixed element f. If x and y are elements of a group $(G, \circ)$, then we say that x *commutes* with y if $x \circ y = y \circ x$.)

Solution to Exercise B121

Here

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Let $g \in S_4$. Then

$$\begin{aligned} &g \circ H \circ g^{-1} \\ &= \{g \circ e \circ g^{-1},\ g \circ (1\ 2)(3\ 4) \circ g^{-1}, \\ &\qquad g \circ (1\ 3)(2\ 4) \circ g^{-1},\ g \circ (1\ 4)(2\ 3) \circ g^{-1}\}. \end{aligned}$$

Now $g \circ e \circ g^{-1} = e$.

Also, we know that

$$g \circ (1\ 2)(3\ 4) \circ g^{-1}$$

is a permutation in S_4 with the same cycle structure as $(1\ 2)(3\ 4)$, so it must be one of the permutations $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$; that is, it must be one of the three non-identity permutations in H. The same argument holds for each of the remaining two conjugates in $g \circ H \circ g^{-1}$.

To complete the proof we have to show that no two of the three permutations

$$\begin{aligned} &g \circ (1\ 2)(3\ 4) \circ g^{-1}, \\ &g \circ (1\ 3)(2\ 4) \circ g^{-1}, \\ &g \circ (1\ 4)(2\ 3) \circ g^{-1} \end{aligned}$$

are equal to the *same* non-identity permutation in H.

This is the case because, by the Cancellation Laws, if x and y are any two elements of S_n, then

$$g \circ x \circ g^{-1} = g \circ y \circ g^{-1}$$

gives $x = y$.

So the four elements of $g \circ H \circ g^{-1}$ are precisely the four elements of H. That is,

$$g \circ H \circ g^{-1} = H.$$

Solution to Exercise B122

(a) The only cyclic subgroup of order 1 is $\{e\}$.

Each cyclic subgroup of order 2 consists of the identity permutation together with one permutation of order 2. Thus the cyclic subgroups of S_4 of order 2 are:

$$\{e,(1\ 2)\},\quad \{e,(1\ 3)\},\quad \{e,(1\ 4)\},$$
$$\{e,(2\ 3)\},\quad \{e,(2\ 4)\},\quad \{e,(3\ 4)\},$$
$$\{e,(1\ 2)(3\ 4)\},\quad \{e,(1\ 3)(2\ 4)\},\quad \{e,(1\ 4)(2\ 3)\}.$$

We now find the cyclic subgroups of S_4 of order 4. The cyclic subgroup generated by the permutation $(1\ 2\ 3\ 4)$ is

$$\begin{aligned}\langle(1\ 2\ 3\ 4)\rangle &= \{e,\ (1\ 2\ 3\ 4), (1\ 2\ 3\ 4)\circ(1\ 2\ 3\ 4),\\ &\qquad (1\ 2\ 3\ 4)\circ(1\ 2\ 3\ 4)\circ(1\ 2\ 3\ 4)\}\\ &= \{e,\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2)\}.\end{aligned}$$

This subgroup contains two permutations of order 4.

We now choose a permutation of order 4 that is not one of these two and find, in the same way as above, the cyclic subgroup that it generates:

$$\langle(1\ 2\ 4\ 3)\rangle = \{e,\ (1\ 2\ 4\ 3),\ (1\ 4)(2\ 3),\ (1\ 3\ 4\ 2)\}.$$

Next we choose a permutation of order 4 that is not one of the four such permutations appearing in the two subgroups of order 4 found already and find the cyclic subgroup that it generates:

$$\langle(1\ 3\ 2\ 4)\rangle = \{e,\ (1\ 3\ 2\ 4),\ (1\ 2)(3\ 4),\ (1\ 4\ 2\ 3)\}.$$

We have now dealt with all six permutations of order 4 in S_4, so we have found all the cyclic subgroups of S_4 of order 4.

(b) The numbers of cyclic subgroups of S_4 of each order can be summarised as follows.

Order	Number of cyclic subgroups
1	1
2	9
3	4
4	3

Solution to Exercise B123

(a) Using the labelling on the figures in the usual way, we obtain the following symmetry groups.

(i) $\{e,(1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}$

(ii) $\{e,\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4\ 3\ 2)\}$

(iii) $\{e,\ (1\ 2)\}$

(iv) $\{e,\ (1\ 3),\ (1\ 4),\ (3\ 4),\ (1\ 3\ 4),\ (1\ 4\ 3)\}$

(b) The subgroups in parts (a)(ii) and (iii) are cyclic, because they are generated by the permutations $(1\ 2\ 3\ 4)$ and $(1\ 2)$, respectively. The other two subgroups are non-cyclic. The subgroup in part (a)(i) has order 4, but contains no element of order 4. The subgroup in part (a)(iv) has order 6, but contains no element of order 6.

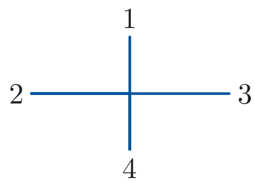
Solution to Exercise B124

(a) We obtain the following subgroup of S_4:

$$\{e,\ (1\ 3),\ (2\ 4),\ (1\ 3)(2\ 4)\}.$$

(You can find the elements of this subgroup either directly from the figure or by renaming the symbols in the permutations in the subgroup found in Exercise B123(a)(i) using the transposition $(2\ 3)$.)

(b) We can relabel the figure as follows.

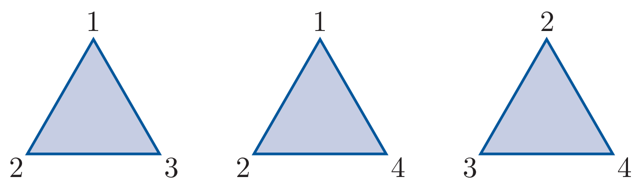


We obtain the following subgroup of S_4:

$$\{e,\ (1\ 4),\ (2\ 3),\ (1\ 4)(2\ 3)\}.$$

Solution to Exercise B125

We can relabel the triangle in the following three ways.

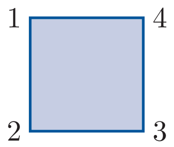


We obtain the following three subgroups of S_4:

$$\{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\},$$
$$\{e,\ (1\ 2),\ (1\ 4),\ (2\ 4),\ (1\ 2\ 4),\ (1\ 4\ 2)\},$$
$$\{e,\ (2\ 3),\ (2\ 4),\ (3\ 4),\ (2\ 3\ 4),\ (2\ 4\ 3)\}.$$

Solution to Exercise B126

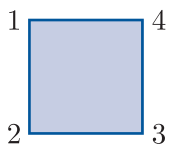
(a) We can use the symmetry group of the square. One way to label the square is as follows.

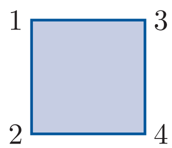


This gives the following subgroup of S_4:

$$\{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2),$$
$$(1\ 4)(2\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)\}.$$

(b) We can relabel the square in the two other ways shown below. In the first we interchange the symbols 2 and 3; in the second we interchange 3 and 4.





We obtain the following two subgroups of S_4:

$$\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3),$$
$$(1\ 4)(2\ 3), (3\ 4), (1\ 3)(2\ 4), (1\ 2)\},$$

$$\{e, (1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2),$$
$$(1\ 3)(2\ 4), (2\ 3), (1\ 2)(3\ 4), (1\ 4)\}.$$

(Notice that although there are other ways of relabelling the vertices of the square, these do not give any more subgroups. For example, interchanging the symbols 1 and 4 leads to the same subgroup as interchanging 2 and 3. In fact we have already found the three subgroups above, at the start of Subsection 4.1.)

Solution to Exercise B127

(a) Not all subgroups of S_4 of order 2 are conjugate to each other.

For example, the subgroups $\{e, (1\ 2)\}$ and $\{e, (1\ 2)(3\ 4)\}$ are not conjugate because the cycle structures of their elements do not match.

(b) All subgroups of S_4 of order 3 are conjugate to each other.

We have seen that the subgroups of S_4 of order 3 are

$$\{e, (1\ 2\ 3), (1\ 3\ 2)\},$$
$$\{e, (1\ 2\ 4), (1\ 4\ 2)\},$$
$$\{e, (1\ 3\ 4), (1\ 4\ 3)\},$$
$$\{e, (2\ 3\ 4), (2\ 4\ 3)\}.$$

The first of these subgroups is conjugated to the other three by, for example, the permutations $(3\ 4)$, $(2\ 4)$ and $(1\ 4)$, respectively. (There are other conjugating permutations, of course.)

Solution to Exercise B128

(a) The subgroup $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$ is the group of direct symmetries of the tetrahedron that fix the vertex at location 2; that is, the group of rotations about an axis passing through the vertex at location 2 and the middle of the opposite face.

(b) The subgroup $\{e, (3\ 4)\}$ is the subgroup generated by the reflection of the tetrahedron in the plane through the edge joining the vertices at locations 1 and 2 and the midpoint of the edge joining the vertices at locations 3 and 4.

(c) The subgroup

$$\{e, (2\ 3), (2\ 4), (3\ 4), (2\ 3\ 4), (2\ 4\ 3)\}$$

is the group of all symmetries of the tetrahedron fixing the vertex at location 1; that is, the group of symmetries of the equilateral triangle with vertices at locations 2, 3 and 4.

(d) The subgroup $\{e, (1\ 2)(3\ 4)\}$ is the subgroup generated by the rotation through π about the line that passes through the midpoint of the edge joining the vertices at locations 1 and 2 and the midpoint of the edge joining the vertices at locations 3 and 4.

Solution to Exercise B129

Using the method of Worked Exercise B47 we obtain the following permutations.

$\circ$	e	a	b	c	p	q	r	s		
e	e	a	b	c	p	q	r	s	$\longrightarrow$	i (identity)
a	a	e	c	b	q	p	s	r	$\longrightarrow$	$(e\ a)(b\ c)(p\ q)(r\ s)$
b	b	c	a	e	r	s	q	p	$\longrightarrow$	$(e\ b\ a\ c)(p\ r\ q\ s)$
c	c	b	e	a	s	r	p	q	$\longrightarrow$	$(e\ c\ a\ b)(p\ s\ q\ r)$
p	p	q	s	r	a	e	b	c	$\longrightarrow$	$(e\ p\ a\ q)(b\ s\ c\ r)$
q	q	p	r	s	e	a	c	b	$\longrightarrow$	$(e\ q\ a\ p)(b\ r\ c\ s)$
r	r	s	p	q	c	b	a	e	$\longrightarrow$	$(e\ r\ a\ s)(b\ p\ c\ q)$
s	s	r	q	p	b	c	e	a	$\longrightarrow$	$(e\ s\ a\ r)(b\ q\ c\ p)$

Hence a permutation group isomorphic to the given group is

$$\{i,\ (e\ a)(b\ c)(p\ q)(r\ s),\ (e\ b\ a\ c)(p\ r\ q\ s),\ (e\ c\ a\ b)(p\ s\ q\ r),\ (e\ p\ a\ q)(b\ s\ c\ r),\ (e\ q\ a\ p)(b\ r\ c\ s),\ (e\ r\ a\ s)(b\ p\ c\ q),\ (e\ s\ a\ r)(b\ q\ c\ p)\},$$

where i is the identity permutation.

Solution to Exercise B130

We have $U_8 = \{1, 3, 5, 7\}$.

We construct the group table for $(U_8, \times_8)$, then from each row we determine, in cycle form, the corresponding permutation of the column headings.

$\times_8$	1	3	5	7		
1	1	3	5	7	$\longrightarrow$	$(1)(3)(5)(7) = e$
3	3	1	7	5	$\longrightarrow$	$(1\ 3)(5\ 7)$
5	5	7	1	3	$\longrightarrow$	$(1\ 5)(3\ 7)$
7	7	5	3	1	$\longrightarrow$	$(1\ 7)(3\ 5)$

Hence a permutation group isomorphic to the group $(U_8, \times_8)$ is

$$\{e,\ (1\ 3)(5\ 7),\ (1\ 5)(3\ 7),\ (1\ 7)(3\ 5)\}.$$

(The group table for $(U_8, \times_8)$ above shows that $(U_8, \times_8)$ has four elements all of which are self-inverse, and hence is isomorphic to the Klein four-group V. So in fact any permutation group isomorphic to V will do as the solution to this exercise, such as the symmetry group of the rectangle when the symmetries are represented as permutations.)